(12) UK Patent Application (19) GB (11) 2 452 688 (13) A

(43) Date of A Publication 18.03.2009

(21) Application No. 0619892.3

(22) Date of Filing: 07.10.2006

(71) Applicant(s):
Andrew Richardson
2 Brookside, DALHAM, Suffolk, CB8 8TG, United Kingdom

Chris Moore
1 Sheepwash Way, Longstanton, CAMBRIDGE, CB4 5GZ, United Kingdom

(72) Inventor(s):
Andrew Richardson
Chris Moore

(74) Agent and/or Address for Service:
Reddie & Grose
16 Theobalds Road, LONDON, WC1X 8PL, United Kingdom

(51) INT CL.
H04W 4/00 (2009.01) ***H04W 4/02*** (2009.01)
H04W 4/04 (2009.01) ***H04W 16/00*** (2009.01)
H04W 28/00 (2009.01) ***H04W 40/00*** (2009.01)
H04W 40/04 (2009.01) ***H04W 80/00*** (2009.01)

(56) Documents Cited:
WO 2008/051124 A1

(58) Field of Search:
INT CL **H04Q, H04W**
Other: **Online : wpi ; epodoc**

(54) Abstract Title: **In-C Device to Core Network Interface Specification**

(57) A 3G access point and a network that the 3G access point connects to. The 3G access point can detect a change in it's location by detecting a change in a measured fingerprint of the local network environment. The fingerprint may be based on neighbouring radio cells, round trip time to target IP nodes or based on the closest location identifier or routing area identifier to the access point.
Also disclosed are a method to ensure handover to the access point in preference to other cells in a cellular network and a method of automatically allocating scrambling codes to access points.

GB 2 452 688 A

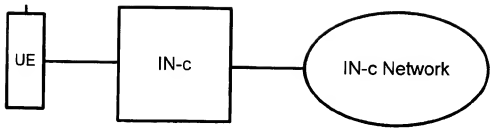


Figure 1: General IN-c Architecture and Interfaces

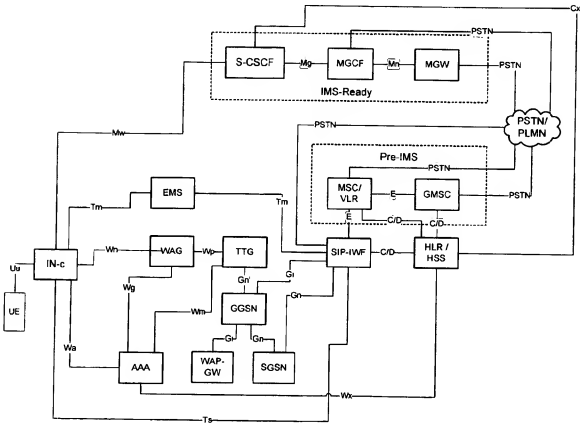


Figure 2 Logical Architecture for IN-c Network

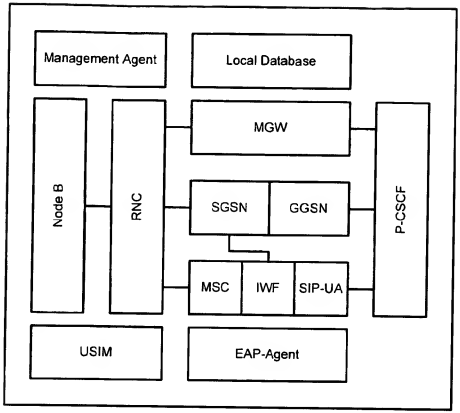


Figure 3 IN-c Device Internal Functional Architecture

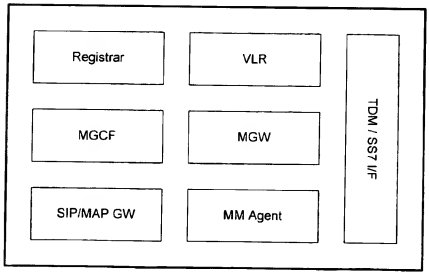


Figure 4 SIP-IWF Internal Functional Architecture

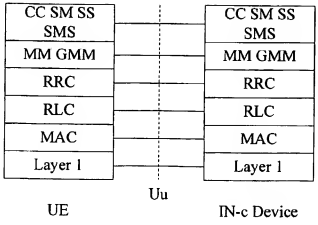


Figure 5: Control Plane UE – IN-c Device

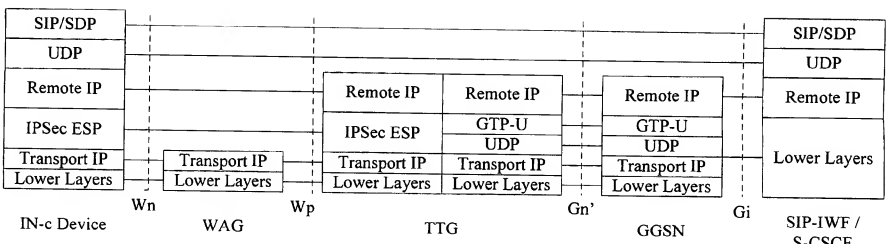


Figure 6: Control Plane IN-c Device – SIP-IWF / S-CSCF

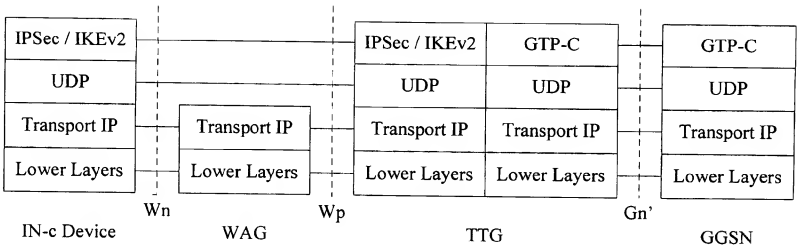


Figure 7 Control Plane IN-c Device – GGSN

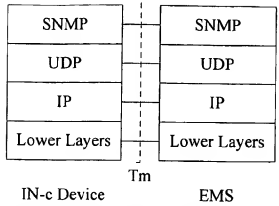


Figure 8: Control Plane IN-c Device – EMS

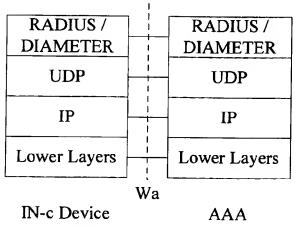


Figure 9: Control Plane IN-c Device – AAA Server

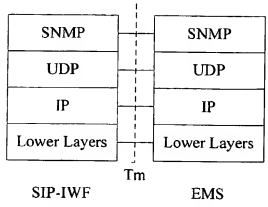


Figure 10: Control Plane SIP-IWF – EMS

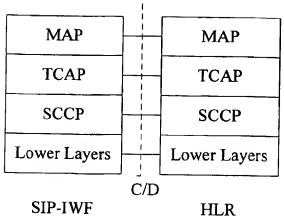


Figure 11: Control Plane SIP-IWF – HLR

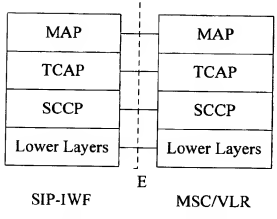


Figure 12: Control Plane SIP-IWF – MSC/VLR

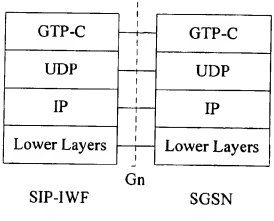


Figure 13: Control Plane SIP-IWF – SGSN

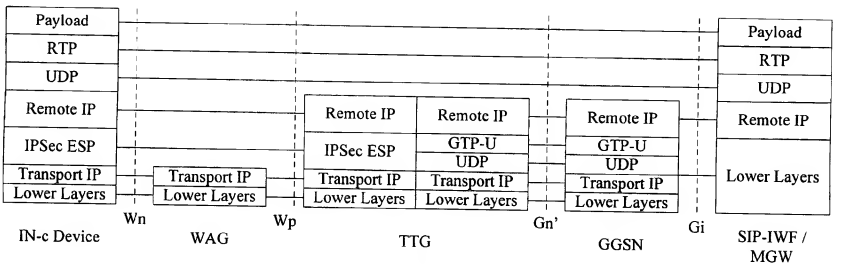


Figure 14: User Plane IN-c Device – SIP-IWF / MGW

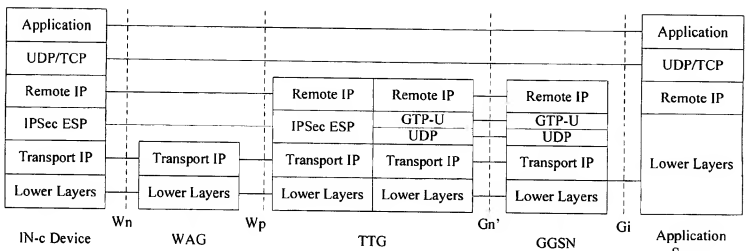


Figure 15: User Plane IN-c Device – GGSN/App Server

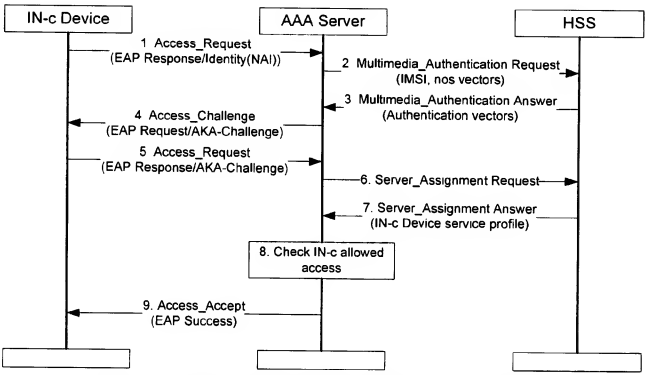


Figure 16: IN-c Device Authentication and Authorisation – RADIUS based

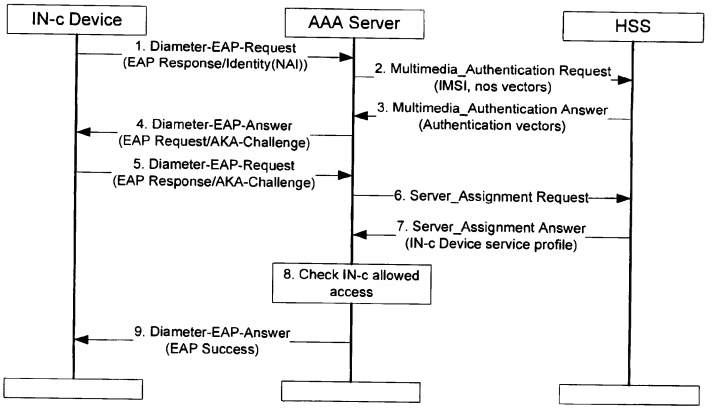


Figure 17: IN-c Device Authentication and Authorisation – DIAMETER based

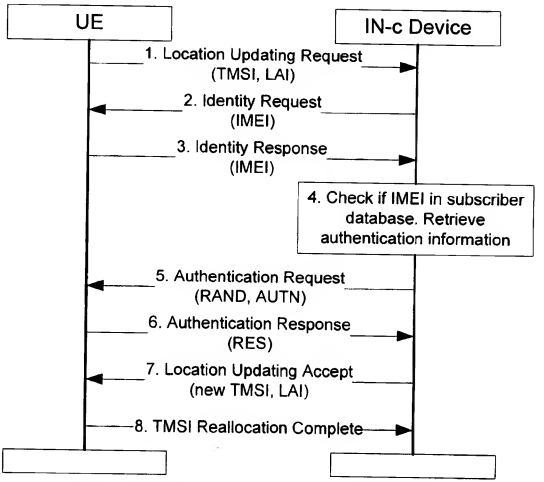


Figure 18: UE Access Controlled by IN-c Device IMEI Known

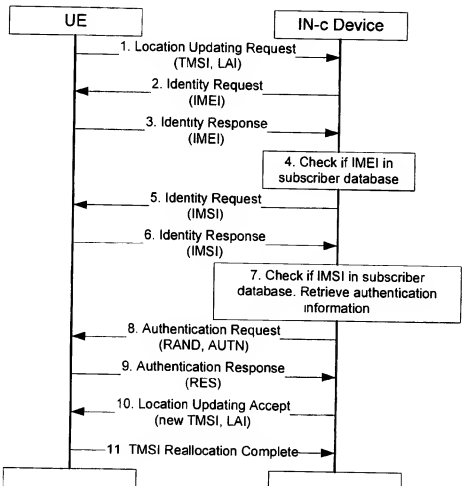


Figure 19: UE Access Controlled by IN-c Device IMEI Unknown

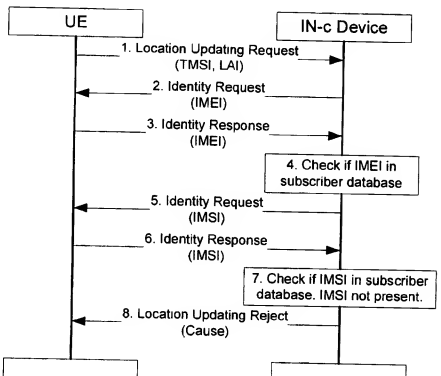


Figure 20: UE Access Controlled by IN-c Device IMSI Unknown

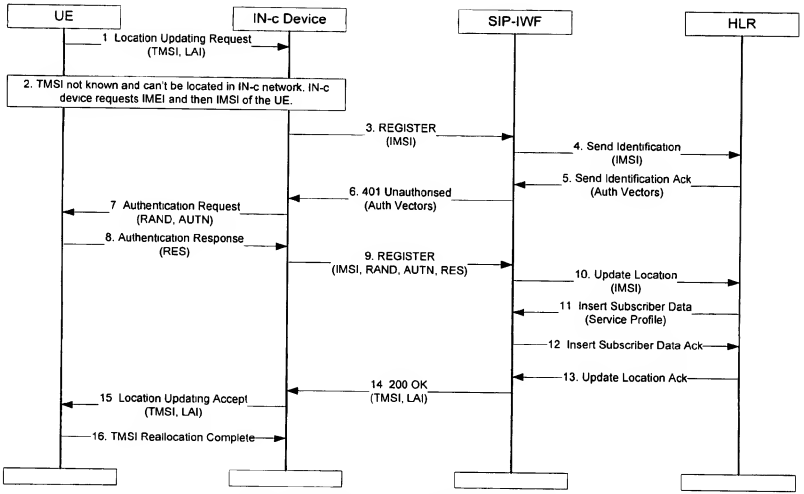


Figure 21: IMSI Attach – Previous PLMN Not Known

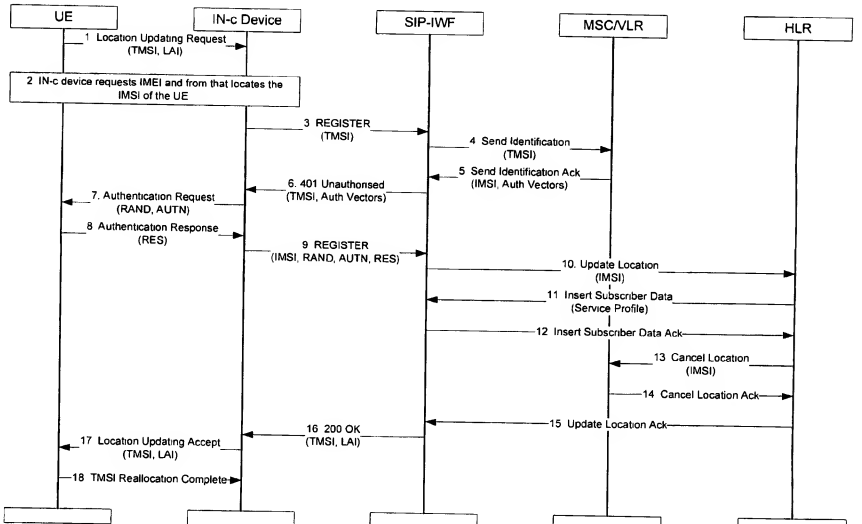


Figure 22: IMSI Attach – Previous PLMN Known

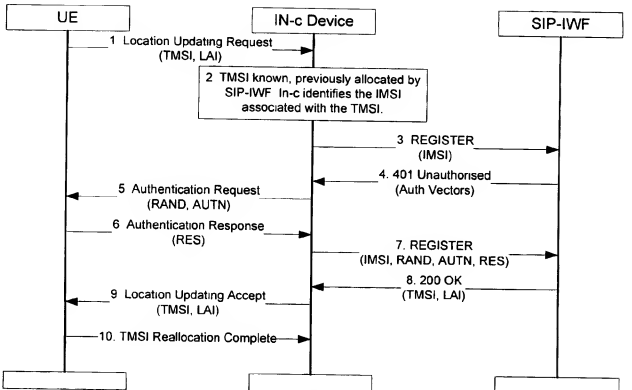


Figure 23: IMSI Attach – Previous Attach to SIP-IWF

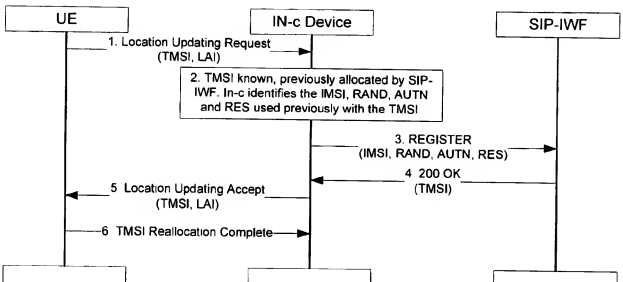


Figure 24: Periodic Location Area Update – Previously Attached to SIP-IWF

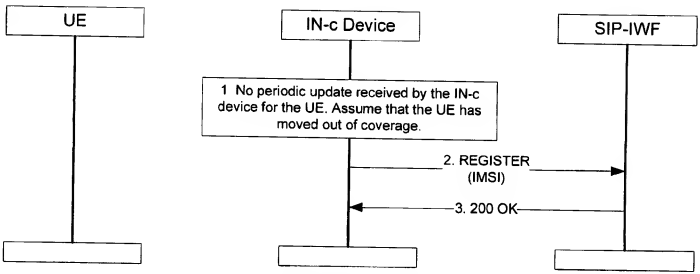


Figure 25: Periodic Update Failed – UE Detached by Network

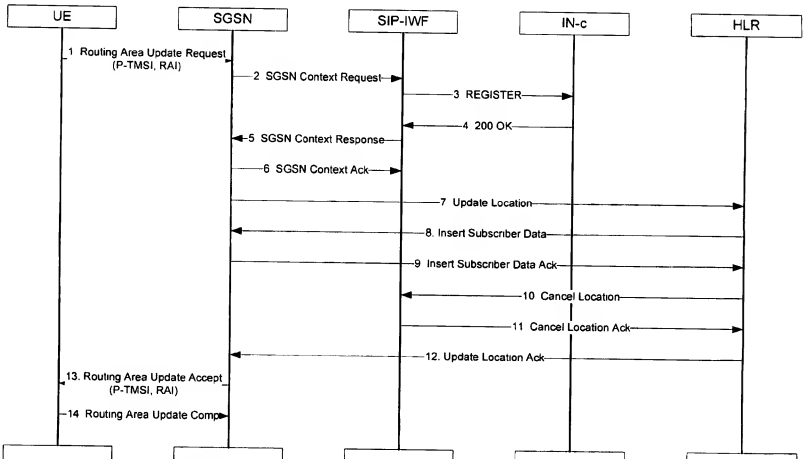


Figure 26: PS Routing Area Update Into Macro Network Using P-TMSI – No PDP Context

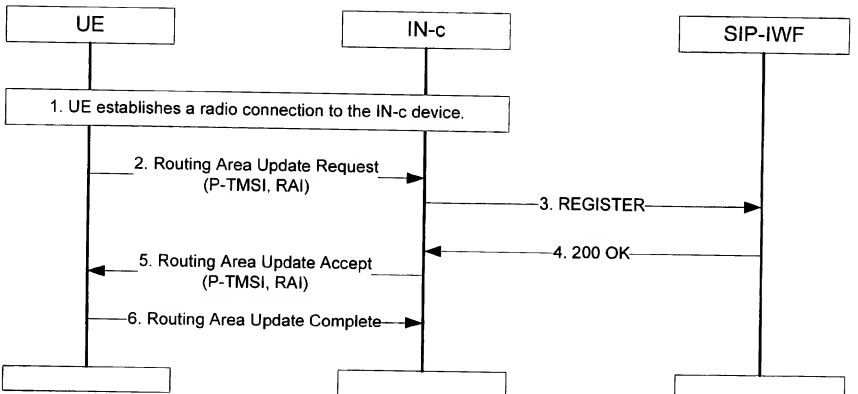


Figure 27: Successful PS Periodic Routing Area Update In IN-c Network – No PDP context

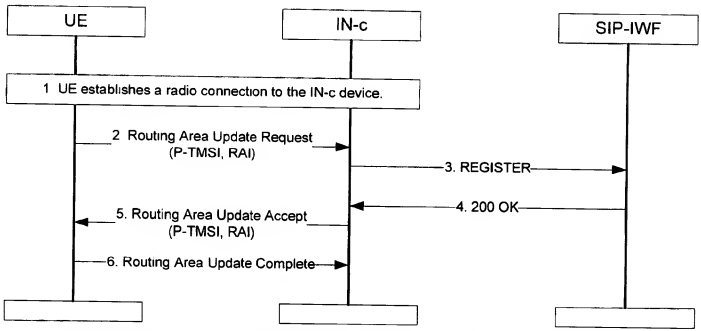


Figure 28: Successful PS Periodic Routing Area Update In IN-c Network – Active PDP Context

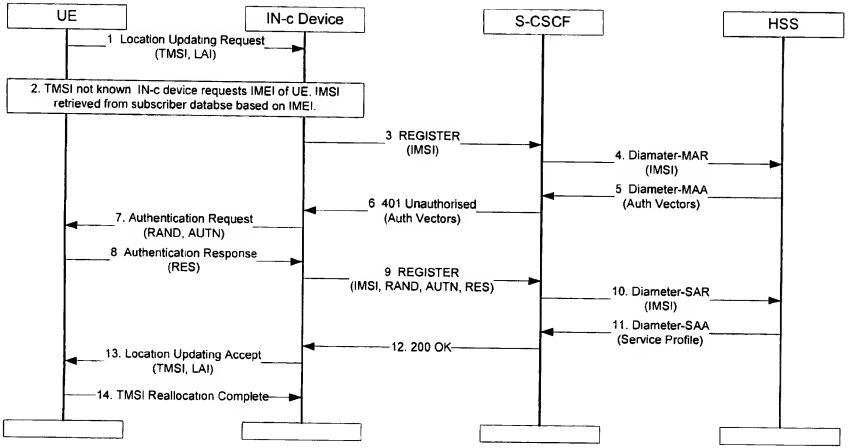


Figure 29: IMS Registration – TMSI Not Known

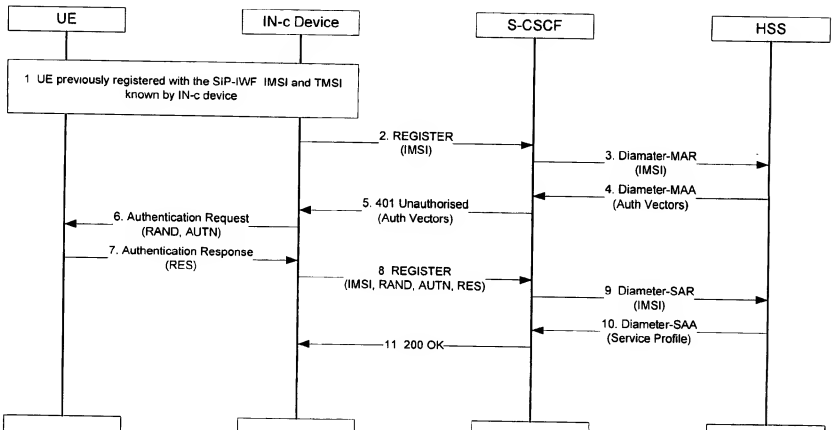


Figure 30: IMS Registration – TMSI Not Known

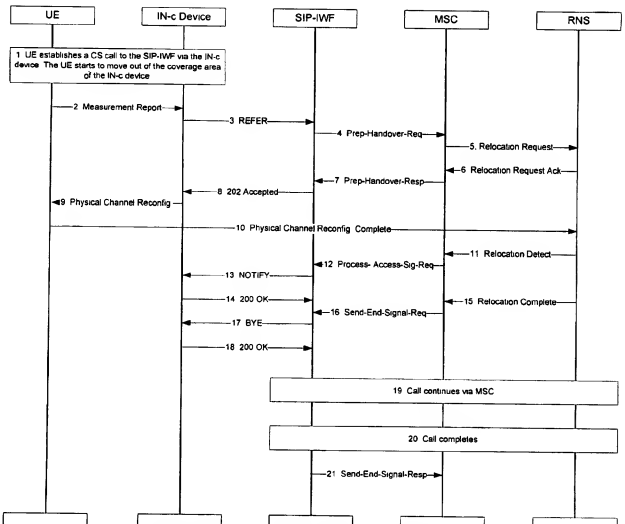


Figure 31: CS Handover from IN-c Device to MSC in Macro Network

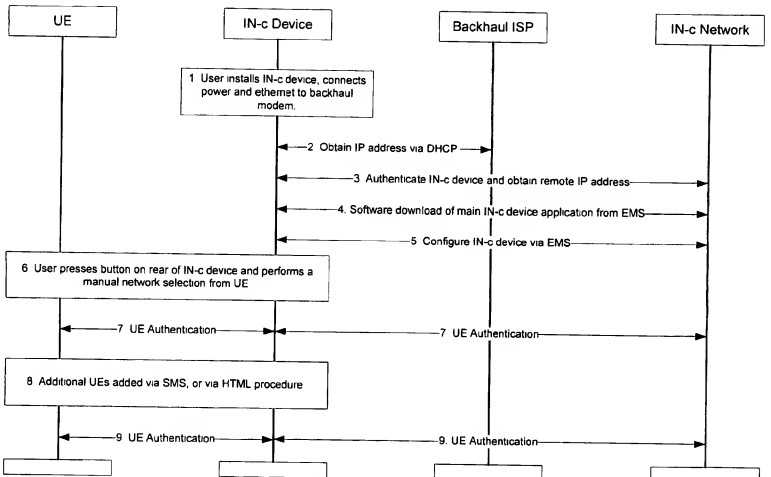


Figure 32: Manual UE Access Control Procedure

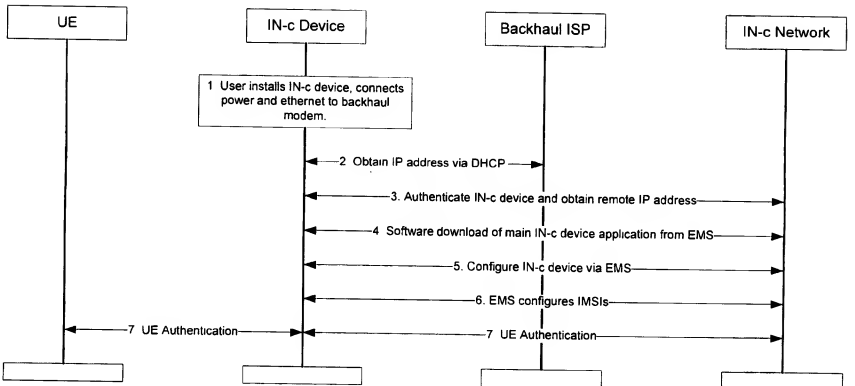


Figure 33: Automatic UE Access Control Procedure

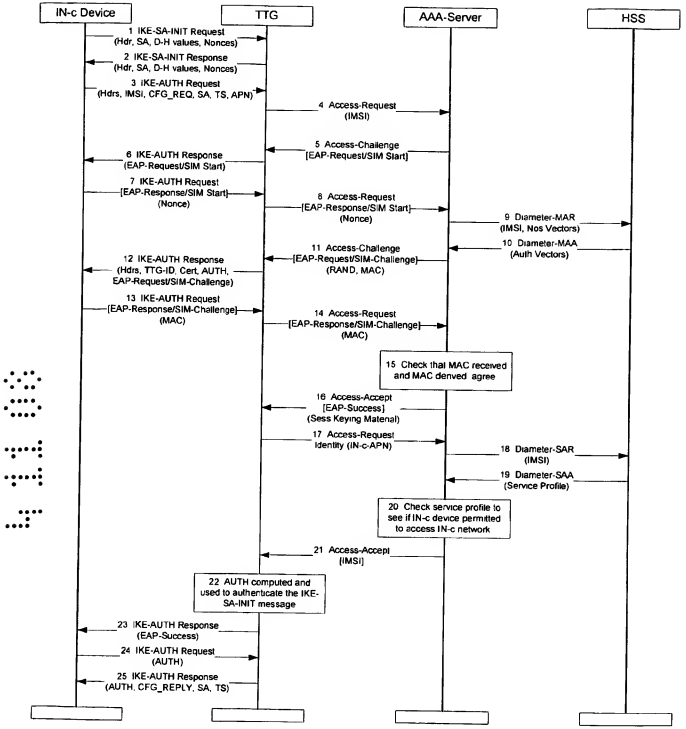


Figure 34: IPSec Tunnel Establishment from IN-c Device to TTG using Radius and EAP-SIM

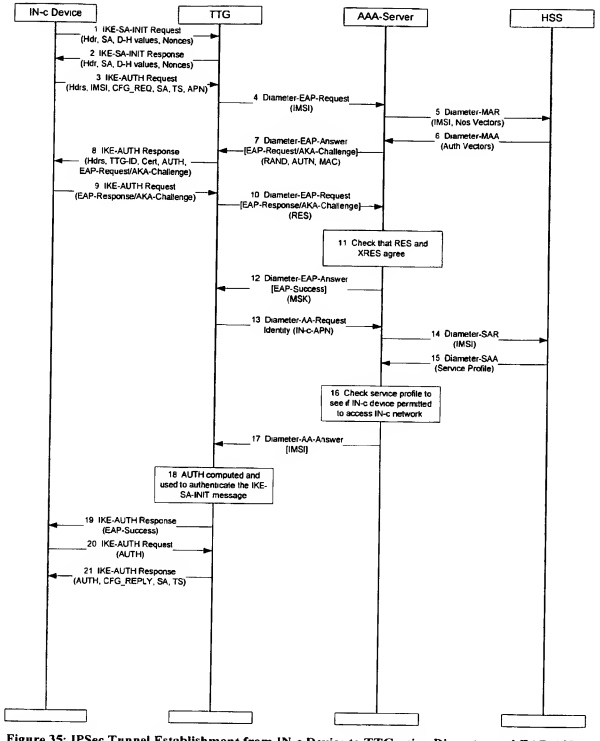


Figure 35: IPSec Tunnel Establishment from IN-c Device to TTG using Diameter and EAP-AKA

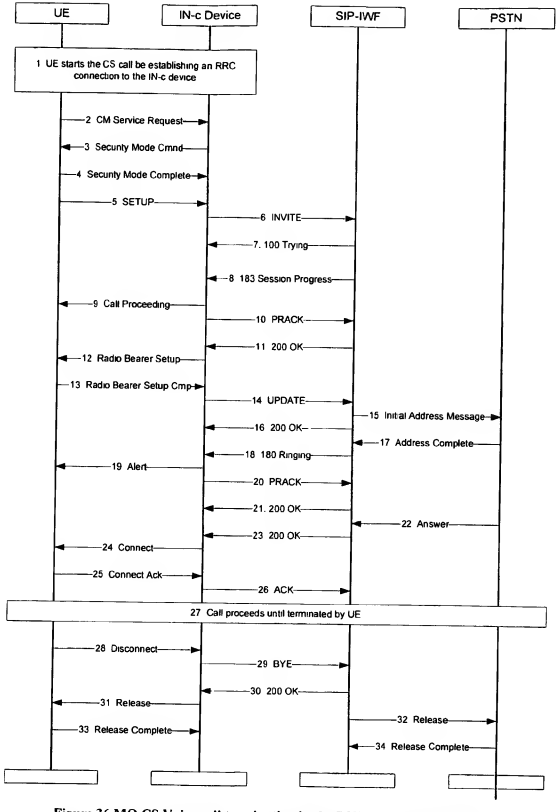


Figure 36 MO CS Voice call terminating in the PSTN – Pre IMS Network

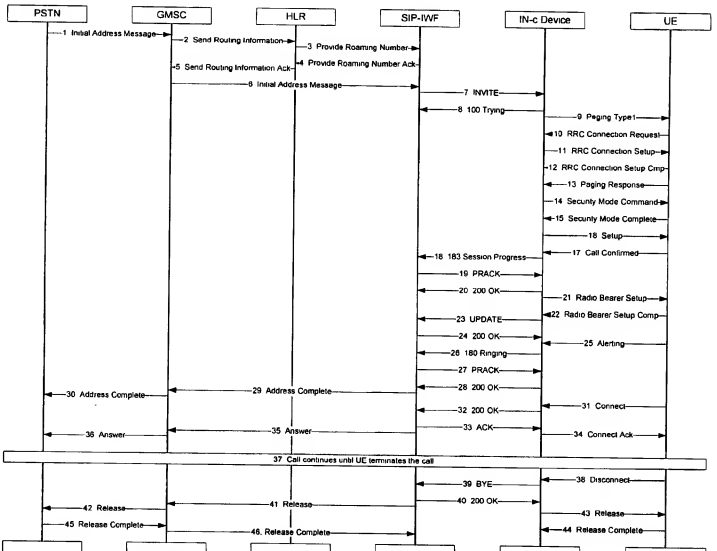


Figure 37: MT CS Voice call originating from the PSTN – Pre IMS Network

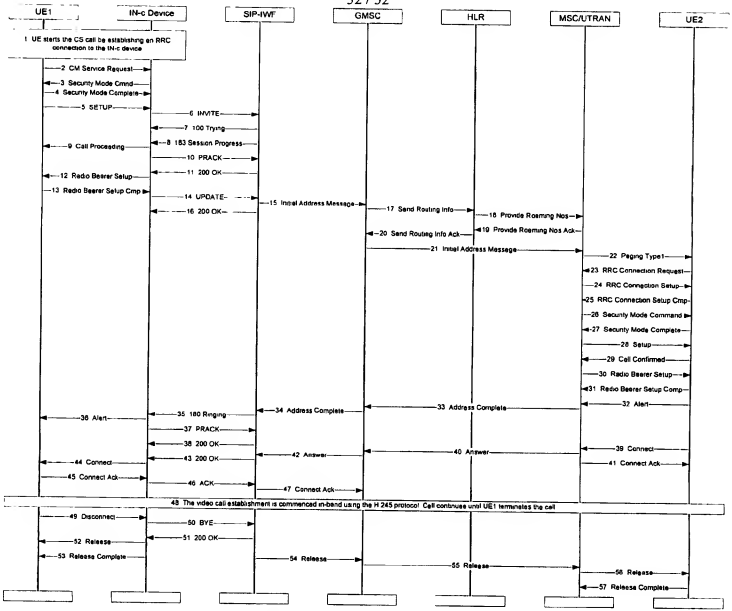


Figure 38: MO CS Video call terminating in a PLMN – Pre IMS Network

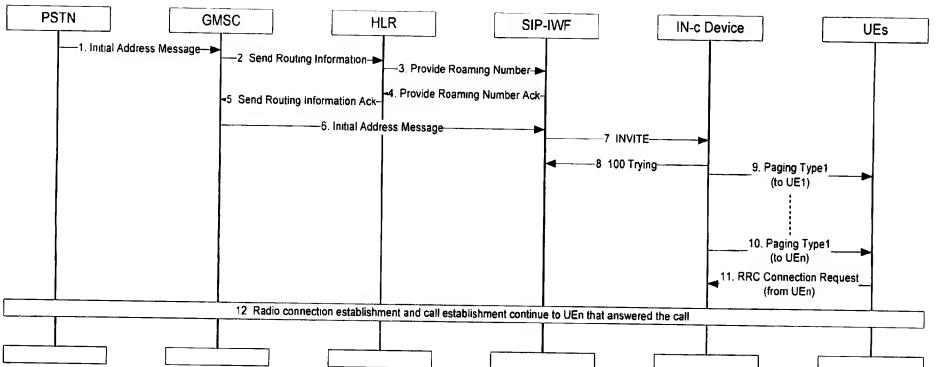


Figure 39: Mobile terminated "Home Call" to the Home Number

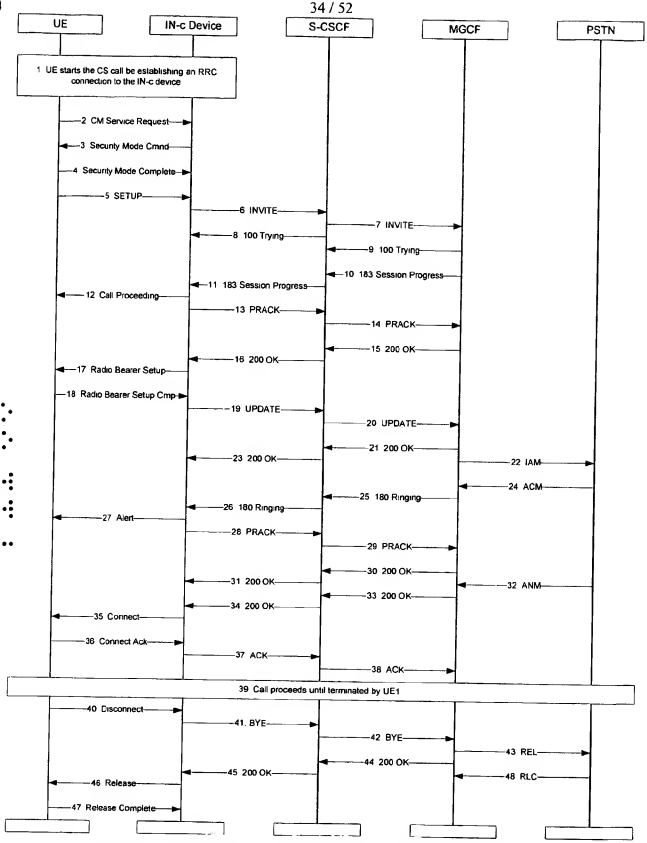


Figure 40: MO CS Voice Call Terminating in the PSTN – IMS-Ready Network

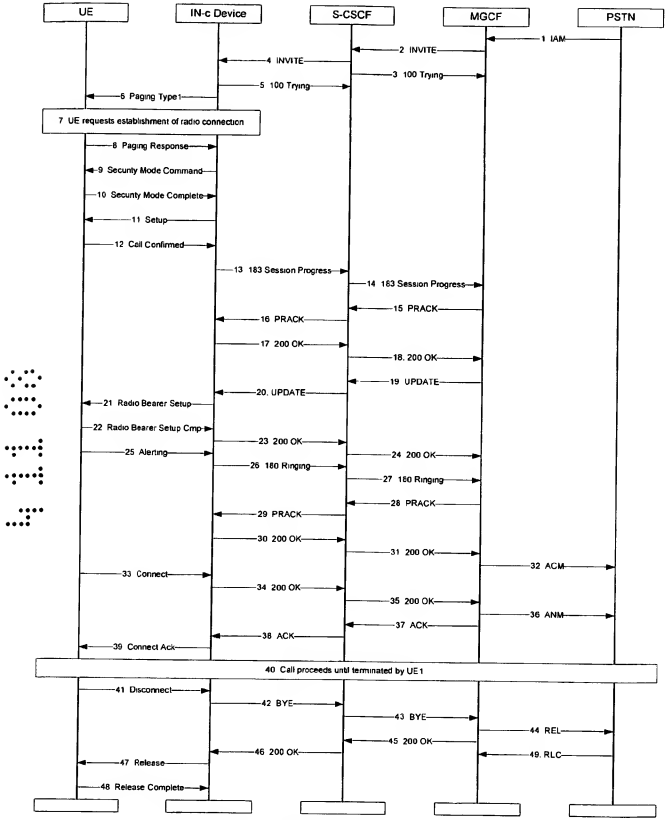


Figure 41: MT CS Voice Call Originating in the PSTN – IMS-Ready Network

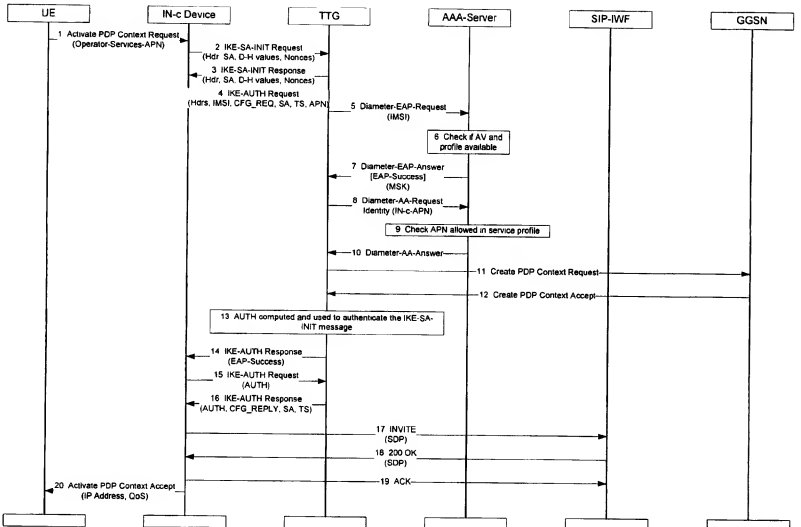


Figure: 42 Packet Data Access to Operator Specific Data Services – Diameter Based

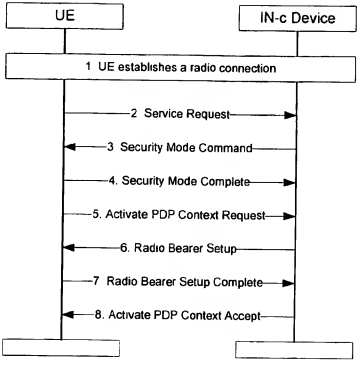


Figure 43: Packet Access to Internet

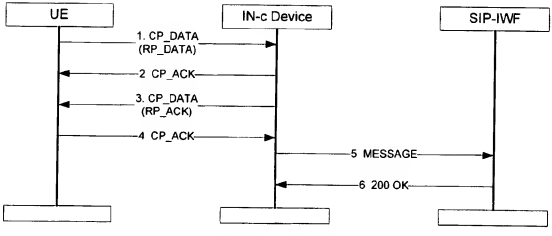


Figure 44: MO SMS Transfer

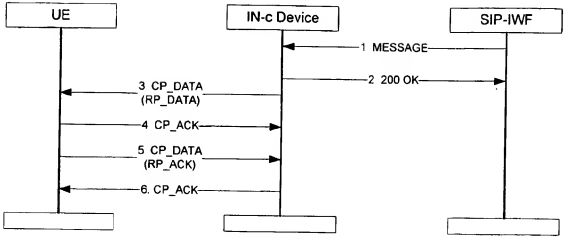


Figure 45: MT SMS Transfer

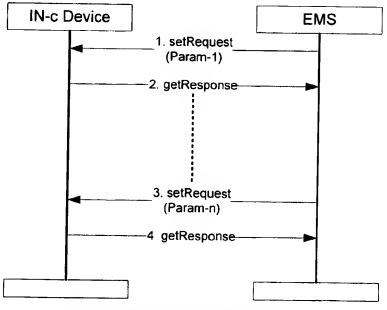


Figure 46: EMS Configuring IN-c Device

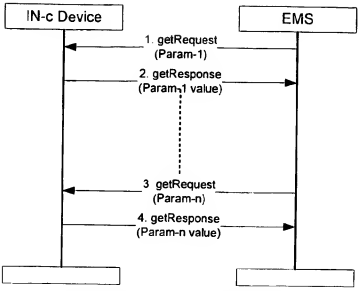


Figure 47: EMS Auditing the IN-c Device

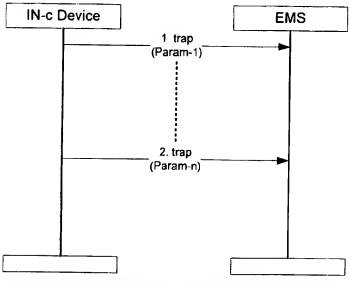


Figure 48: Error and Event Reporting in IN-c Device

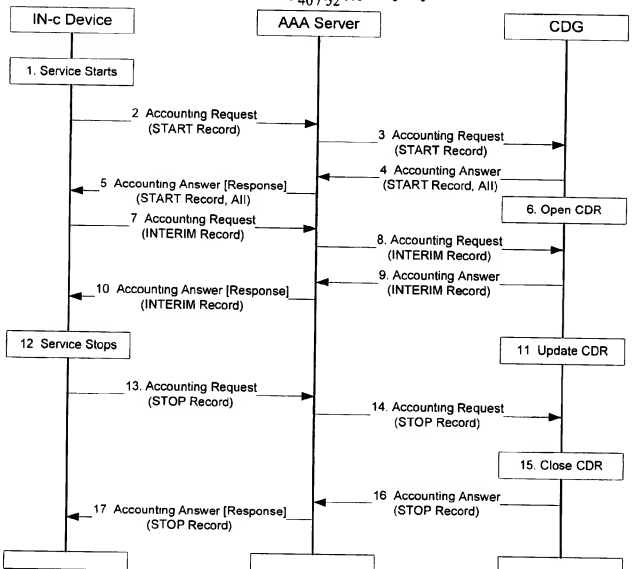


Figure 49: IN-c Device Derived Charging Message Flows Based on DIAMETER and RADIUS

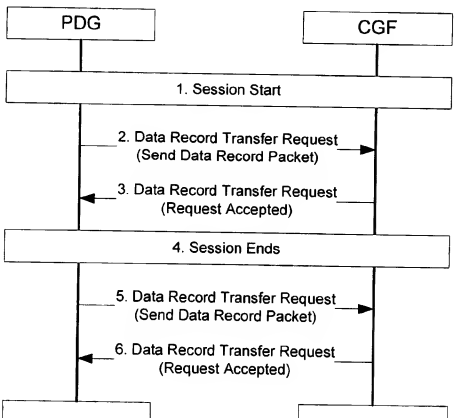


Figure 50: PDG Derived Charging Message Flows

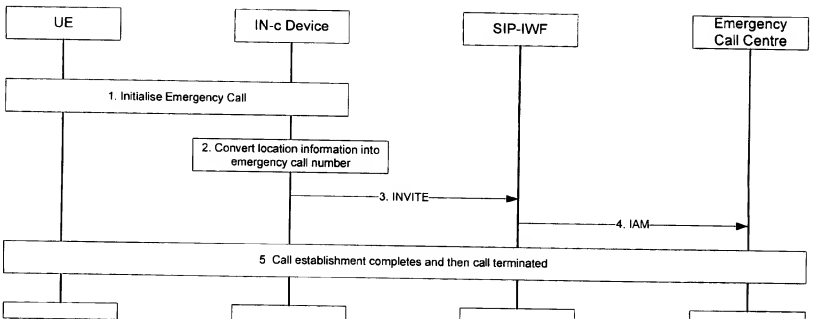


Figure 51: Emergency Call Via SIP-IWF

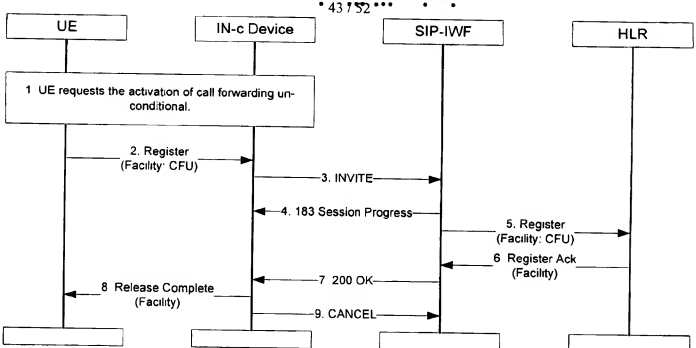


Figure 52: Call Forwarding Unconditional Activation

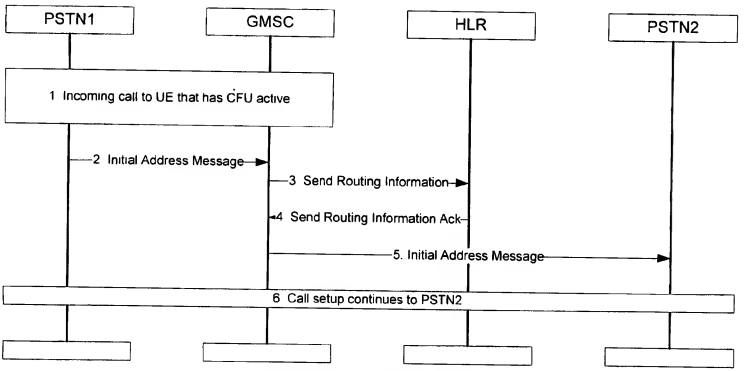


Figure 53: Example Call Forwarding

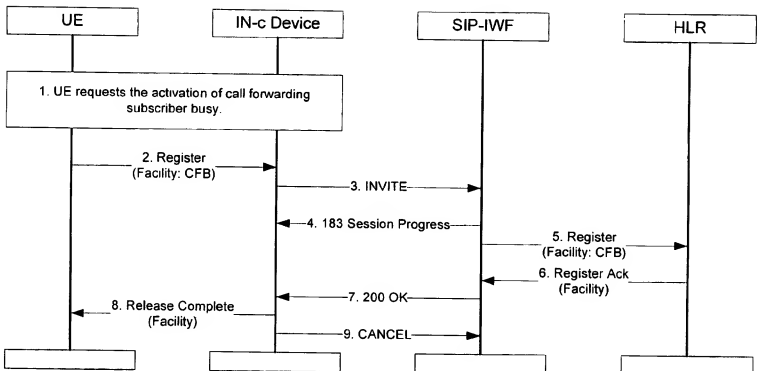


Figure 54: Call Forwarding on Mobile Subscriber Busy Activation

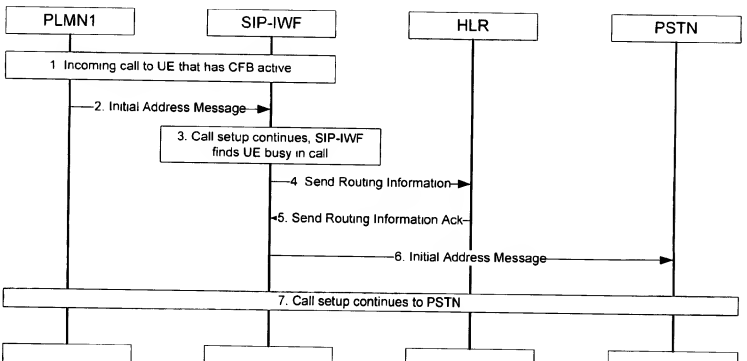


Figure 55: Example Call Forwarding on Mobile Subscriber Busy

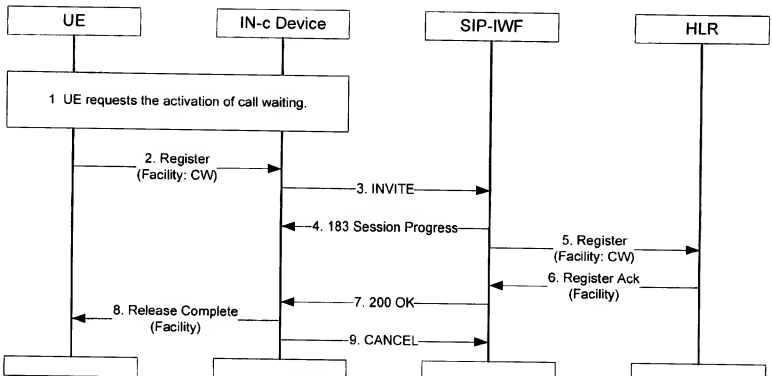


Figure 56: Call Waiting Activation

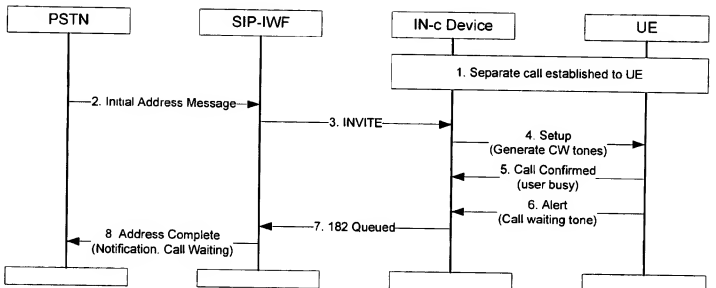


Figure 57: Call Waiting Example

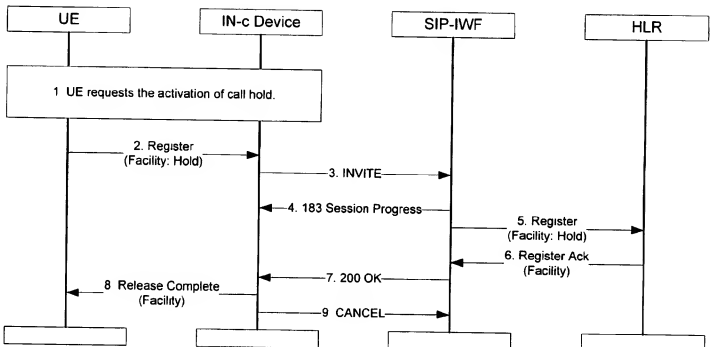


Figure 58: Activation of Call Hold

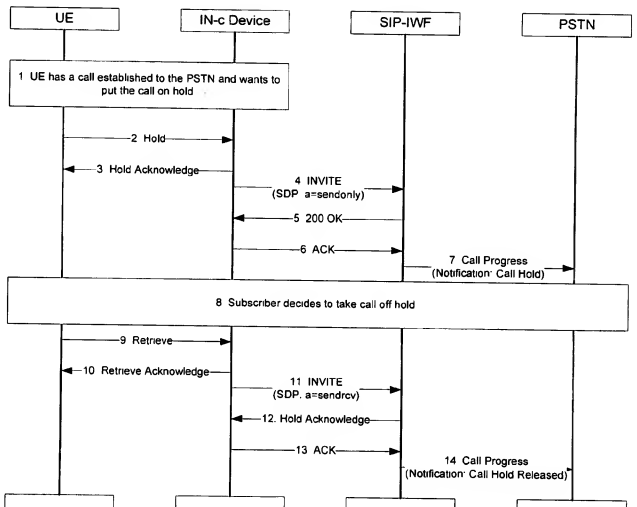


Figure 59: Call Hold Example

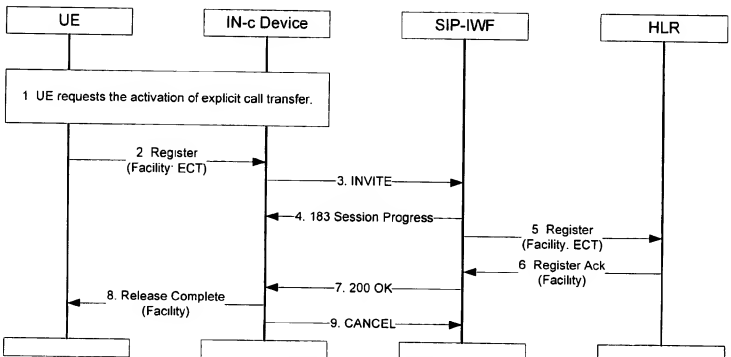


Figure 60: Activation of Explicit Call Transfer

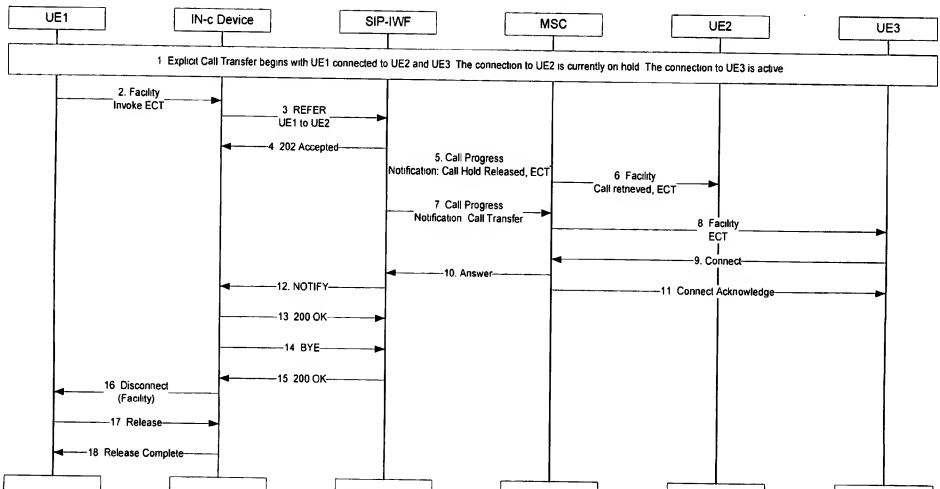


Figure 61: Example of Explicit Call Transfer

1. Introduction

To satisfy the requirements for residential access to 3G services this document proposes a 3G access point and a network that the 3G access point connects to. The 3G access point is called an IN-c (Integrated Network on a card) device and the network that the access point connects to, the IN-c network.

The purpose of this document is to define the functions that exist within the IN-c device, the functions that exist in the IN-c network, and the interface that exists between the IN-c device and the IN-c network. For use in the home environment, the IN-c device is also referred to as a Home Base Station (HBS).

The IN-c device will be a new network entity that is manufactured either by 3Way Networks or by a licensed technology partner. The IN-c device is a small low power CPE that is used for residential access to an operator's 3G services.

The IN-c network is the operators existing PLMN, but with some additional network elements that are required to support certain requirements of the IN-c device. The operators existing network may be either a 3GPP Release 99 compliant network or it may be a 3GPP Release 5/6 IMS based network; here these are referred to as a pre-IMS or an IMS-ready architecture, respectively.

1.1 Scope

This document describes the stage 2 features, functions and message flows between the IN-c device and the IN-c network for the requirements defined in [2]. The document will not consider the detail of the procedures that exist outside of these network entities or the interface we are considering.

1.2 References

[1] IN-c Device to Core Network Interface Document: Stage 3 Specifications, 3Way Networks

[2] HBS to Core Network Interface Document – Stage 1 Requirements, 3Way Networks

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[5] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[6] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[7] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[8] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[9] 3GPP TS 23.002: Network Architecture

[10] 3GPP TS25.104 Tx and RX specs

[11] 3GPP TS 23.206 VCC

[12] RFC 2138 - Remote Authentication Dial In User Service (RADIUS)

[13] RFC 3588 Diameter Base Protocol

[14] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description; Stage 2"

[15] RFC 1157 - Simple Network Management Protocol (SNMP)

[16] DSL Forum TR-069, "CPE WAN Management Protocol"

[17] www.osgi.org

[18] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2"

[19] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[20] 3GPP TS 25.331: "RRC Protocol Specification".

[21] 3GPP TS 25.322: "RLC protocol specification".

[22] 3GPP TS 25.321: "Medium Access Control (MAC) protocol specification".

[23] 3GPP TS 25.323: "Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 25.201: "Physical layer - general description".

[25] RFC 3267: "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs"

[26] RFC 3550: "RTP: A Transport Protocol for Real-Time Applications"

[27] RFC 768: "User Datagram Protocol"

[28] RFC 791: "Internet Protocol"

[29] RFC 4303: "IP Encapsulating Security Payload (ESP) "

[30] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[31] RFC 3261: "SIP: Session Initiation Protocol".

[32] RFC 4566: "SDP: Session Description Protocol".

[33] RFC 2401: "Security Architecture for the Internet Protocol"

[34] RFC 4306: "Internet Key Exchange (IKEv2) Protocol"

[35] 3GPP TS 29.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description; Stage 3".

[36] RFC 3579: "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)".

[37] RFC 4186: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)".

[38] RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[39] RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[40] 3GPP TS 33.102: "3G security; Security architecture".

[41] draft-ietf-aaa-diameter-sip-app-12 "Diameter Session Initiation Protocol (SIP) Application"

[42] RFC 4005: "Diameter Network Access Server Application"

[43] ETSI TS 183 043: "Protocols for Advanced Networks (TISPAN); IMS-based PSTN/ISDN Emulation Stage 3 specification"

[44] RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

2. Definitions, abbreviations and symbols

2.1 Definitions

IN-c device: The IN-c device is the physical units that are deployed as CPE in the subscribers residence or place of work.

IN-c network: The IN-c network is all of the network elements that are required to allow the IN-c device to function according to this specification. The IN-c network does not imply that these are new network elements, most of the elements of the IN-c network already exist within the operator's PLMN.

Pre-IMS network: A PLMN network that does not support the 3GPP IMS functions defined in [6].

IMS-Ready Network: A PLMN network that does support the 3GPP IMS functions defined in [6].

2.2 Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorisation and Accounting
ACM	Address Complete
AF	Assured Forwarding
AICH	Acquisition Indication Channel
AKA	Authentication and Key Agreement
AMR	Adaptive Multi Rate
API	Application Programming Interface
APN	Access Point Name
ARFCN	Absolute Radio Frequency Channel Number
AUTN	Authentication Token
BCCH	Broadcast Control Channel
BCC	BCCH Colour Code
BE	Best Efforts
BSIC	Base Station Identity Code

CC	Call Control
CDF	Charging Data Function
CDR	Charging Data Record
CPE	Customer Premises Equipment
CPICH	Common Pilot Channel
CS	Circuit Switched
D-H	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DPCCH	Dedicated Physical Control Channel
DPDCH	Dedicated Physical Data Channel
DSCP	DiffServ Code Point
DSL	Digital Subscriber Loop
EAP	Extensible Authentication Protocol
E-CSCF	Emergency Call Session Control Function
EF	Expedited Forwarding
EMS	Element Management System
ESP	Encapsulating Security Payload
FFS	For Further Study
FTP	File Transfer Protocol
HPLMN	Home PLMN
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HS-DPCCH	High Speed Dedicated Physical Control Channel
HS-PDSCH	High Speed Physical Downlink Shared Channel
HSS	Home Subscriber Server
HS-SCCH	High Speed Shared Control Channel
IAM	Initial Address Message
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem
IN-c	Integrated Network on a card
IP	Internet Protocol
IPSec	IP Security

ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IWF	Inter-Working Function
GGSN	Gateway GPRS Support Node
GMM	GPRS Mobility Management
GMSC	Gateway Mobile Switching Centre
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GTP-C	GPRS Tunnelling Protocol – Control Plane
GTP-U	GPRS Tunnelling Protocol – User Plane
LAC	Location Area Code
LAI	Location Area Identifier
MAA	Multimedia Authentication Answer
MAC	Message Authentication Code
	Medium Access Control
MAP	Mobile Application Part
MAR	Multimedia Authentication Request
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway
MIB	Management Information Base
MM	Mobility Management
MNC	Mobile Network Code
MO	Mobile Originated
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN Number
MSK	Master Session Key
MT	Mobile Terminated
NAI	Network Access Identifier
NAT	Network Address Translation
NCC	Network Colour Code
OAM	Operations and Maintenance
OSGi	Open Services Gateway Initiative
PCM	Pulse Code Modulation

P-CCPCH	Primary Common Control Physical Channel
P-CPICH	Primary CPICH
P-CSCF	Proxy Call Session Control Function
PDCP	Packet Data Control Protocol
PDG	Packet Data Gateway
PDN	Packet data Network
PDP	Packet Data Protocol
PHB	Per-Hop Behaviour
PLMN	Public Land Mobile Network
PRACH	Physical Random Access Channel
PS	Packet Switched
QoS	Quality of Service
RAB	Radio Access Bearer
RAC	Routing Area Code
RADIUS	Remote Authentication Dial In User Service
RAI	Routing Area Identifier
RANAP	Radio Access Network Application Part
RAND	Random number
RAT	Radio Access Technology
RES	Response
REL	Release
RF	Radio Frequency
RLC	Radio Link Control
	Release Complete
RNC	Radio Network Controller
RRC	Radio Resource Control
RRM	Radio Resource Manager
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTT	Round Trip Time
RSCP	Received Signal Code Power
SA	Security Association
SAA	Server Assignment Request
SAR	Server Assignment Answer

SCCP	Signalling Connection Control Part
S-CCPCH	Secondary Common Control Physical Channel
SCH	Synchronisation Channel
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SFN	System Frame Number
SIB	System Information Block
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SM	Session Management
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SoHo	Small Office Home Office
SPI	Security Parameter Index
SRB	Signalling Radio Bearer
SS	Supplementary Service
SS7	Signalling System Number 7
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TMSI	Temporary Mobile Subscriber Identity
TS	Traffic Selector
TTG	Tunnel Termination Gateway
UA	User Agent
UARFCN	UTRAN Absolute Radio Frequency Channel Number
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VCC	Voice Call Continuity
VLR	Visitor Location Register

WAG	Wireless Access Gateway
WAMR	Wideband AMR
WCDMA	Wideband Code Division Multiple Access

2.3 Symbols

AUTN	Authentication Token
RAND	Random Number
RES	Response
XRES	Expected Response

2.4 List of Interfaces

Gn	GGSN to SGSN
Gi	GGSN to PDN
Uu	UE to IN-c device
Wa	GGSN

3. General IN-c Architecture and Transmission Mechanism

3.1 IN-c Access Interfaces and Reference Points

The general architecture for the inter-connection of the IN-c device, the IN-c network and a UE are illustrated in Figure 1. This is a high level architecture diagram, a more detailed logical architecture is considered later.

3.1.1 UE

The User Equipment (UE) shall meet 3GPP R99 and later specifications. There are no additional requirements for the specification of the UE other than those that define the services that the subscriber hopes to gain from the IN-c device and the IN-c network. For example, should a subscriber wish to gain access to the HSDPA services of the IN-c network via the IN-c device, that UE shall support the appropriate 3GPP specifications that define the operation for HSDPA access.

If the UE is 3GPP Release 6 IMS compliant, the IN-c device will operate the UE in its Release 99 mode of operation across the radio interface for circuit switched services such as voice and video.

The number of UEs that a specific IN-c device can support is an implementation decision, but typically will be less than ten per IN-c device.

3.1.2 IN-c Device

The IN-c device is the CPE that is located in the subscriber's residence. The IN-c device provides a range of functions such as registration, authentication, service establishment and control, billing and security. The detailed functions of the IN-c device are considered in a later section.

3.1.3 IN-c Network

The IN-c device shall connect to the IN-c network. The physical connection between the IN-c device and the IN-c network may be over a range of different technologies (e.g. xDSL, cable or satellite). The transport requirements for this connection are considered later.

The IN-c network illustrated in Figure 1 is compromised of many elements. The IN-c network is based on an operators existing PLMN infrastructure, to which some new network elements are added to facilitate the interworking with the IN-c device.

The existing PLMN infrastructure elements can be either pre-IMS (Release 99) or IMS ready (3GPP Release 5/6). In either case the IN-c device is designed to work with both network variants. Some of the PLMN network elements are independent of whether it is a pre-IMS or an IMS ready network. There are some new network components required. These are described below.

3.1.3.1 IMS Independent Network Elements

There are a number of elements in the IN-c network that are independent on whether the IMS has been deployed or not These elements may include network entities such as the billing systems, the OAM systems, many parts of

the UTRAN and even elements in the packet domain such as the SGSN and the GGSN.

3.1.3.2 Pre-IMS - Network Elements

The networks that are pre-IMS shall be based on the 3GPP Release 99 specifications and include network entities such as MSCs, GMSCs and VLRs as well as the HLR. The IN c device will interoperate with these network entities to facilitate the establishment of services such as voice, video and SMS using the standard set of protocols.

To support the operation of the IN-c device in a pre-IMS network, a number of new infrastructure components are required and described below.

3.1.3.3 IMS-Ready - Network Elements

The IN-c device will operate with an IMS ready network. In this instance, the IN-c device takes the role of the P-CSCF within the IMS network for the specific services that are originated through the IN-c device. To inter-operate with the IN-c device and the IMS-ready network, the UE may be either R99 compliant, R5 or later.

To support the operation of the IN-c device within an IMS-ready network a number of additional network elements are included. These network elements are outlined described below.

3.1 3.4 New Network Elements

To support the IN-c device in either a pre-IMS network or an IMS-ready network there are a number of new network elements that are required. Some of these new network elements are common to both the pre-IMS and IMS-ready architectures and some are specific to that architecture.

The new network elements are present to handle a range of functions that arise when the IN-c device is attached to the operators PLMN. These functions include access security, access control, mobility management and

billing. An overview of these functions is considered in the following section and in more detail later.

3.2 High-Level Functions

The following list provides the high level functions that are required in the IN-c device and the IN-c network No assumptions as to the topology of the IN-c network architecture have been made. The differences between the different network architectures will be highlighted in the later sections when we consider the detail inter-operation of the IN-c device and IN-c network.

- Access Control and Registration Functions.
- Packet Routeing and Transfer Functions.
- Call / Session Establishment Functions.
- Mobility Management Functions.
- Radio Resource Management Functions.
- Network Management Functions.
- Billing and Charging Functions.
- Security Functions.
- Emergency Call Functions.
- QoS Functions.
- Software Download Functions.
- Lawful Intercept Functions
- Location Awareness Functions
- Prevention of Roaming Fraud Functions

3.2.1 Access Control and Registration Functions.

The access control functions are the means through which access to the IN-c network is controlled. The access control is applied to the UEs that are accessing the IN-c network and the IN-c devices themselves.

The IN-c devices shall connect to the operator's core network (IN-c network). Access control shall be applied to the IN-c device to ensure that only valid IN-c devices are allowed to access the operators IN-c network.

Access control of the UE to the IN-c network shall be applied. The UE access control is composed of two aspects:

The first aspect of UE access control shall control which UEs are allowed to access a specific IN-c.

The second aspect of UE access control shall control the access the IN-c network via the IN-c device.

3.2.1.1 IN-c Device - Access Control Function

Before gaining access to the operator's IN-c network, the IN-c device shall perform registration, authentication and authorisation functions. The registration function is performed to notify the IN-c Network that the IN-c device is present, the authentication function is performed to ensure that the IN-c device is authentic and the authorisation function is performed to ensure that the IN-c device is authorised to access the IN-c network.

The cryptographic algorithms used in the registration and authentication procedures may be defined by the operator.

3.2.1.2 IN-c Device – UE Access Control Function

In the home environment, the IN-c device may have low capacity and have restrictions over the backhaul bandwidth. To ensure that the owner of the IN-c device in the home retains control over which UEs can access that specific IN-c device, access control is present in each IN-c device, and a database used to define which UEs are permitted to access that specific IN-c. The gating on which devices are allowed is operator definable and based on either the IMSI or the IMEI.

Two mechanisms are defined for controlling the access to the IN-c device. One mechanism allows the end user to control access and in the second mechanism it is the operator that controls access. It will be an operator configurable option as to which of the two mechanisms are allowed.

To support the end-user control of access to the IN-c device, the concept of a master user is introduced. A procedure is defined to allow a user to be registered as the master user on the IN-c device. Once the master user is defined, they shall control access of other users via a simple configuration procedure.

For the operator defined access control, the configuration data on which IMSIs are allowed to access the IN-c device are configured via the EMS and downloaded to the IN-c device when the IN-c device is configured and periodically thereafter.

3.2.1.3 IN-c Network - Registration Function

When the UE has gained access to the IN-c device in the home, they shall request access to the IN-c network. This procedure allows the network operators to control access based on IMSI and registration status. The procedures to control access to the IN-c network are based on standard 3GPP authentication and registration procedures. The authentication algorithms are defined and controlled by the operator.

3.2.2 Packet Routeing and Transfer Functions

3.2.2 1 Internal Network Data Routing Function

The internal network data routing function determines the path that the data packets shall take within the network and allows access to operator specific data services. The access to the operator specific services will be based on user subscription and so the routing functions will be gated based on the state of that subscription.

The operator will control both the availability of the internal network data routing and also the individual subscriber access to these services.

Billing records shall be created for the access to the internal data network.

3.2.2.2 External Network Data Routing Function

The external network data routing function shall allow access to non-operator data services such as the Internet The routing to the internet will be via the first available route, most likely in the transport network. The operator shall control the access to these external data networks.

Billing records shall be created for the access to the external data network.

3.2.2.3 NAT Function

Network Address Translation (NAT) is a mechanism that is used to convert an address of one type to a different address that is either the same or a different type.

Within the IN-c network there may be a requirement to select addresses based on the availability of the sub-net addresses of the different parts of the network. NAT functions will be used within the network to manage the changes in these addresses.

3.2.2.4 Tunnelling Function

The tunnelling function consists of the encapsulation of data packets from the point where they are encapsulated to the end-point where they are de-encapsulated. The tunnelling overcomes some of the issues to do with the addressing space in which the end-points are located and also provide a mechanism to enhance the security of the links between the end-points.

Within the IN-c network tunnelling is used from the IN-c device to elements within the IN-c network.

3.2.2.5 Compression Function

The compression function is used to optimise the transmission resources between the IN-c device and the elements within the IN-c network. The compression function can be used to compress signalling data, user data and the data packet header information. Between the IN-c device and elements within the IN-c network, only the compression of the data packet headers is

supported. Future versions of this document may support compression of the signalling data.

3.2.2.6 Ciphering Function

The ciphering function provides confidentiality of the user data and signalling. The interface between the IN-c device and the IN-c network will be ciphered.

3.2.3 Call / Session Establishment Function

The call and session establishment functions are those functions that are required to establish and support CS services such as voice and video services as well as packet sessions.

The interface specification between the IN-c device and the IN-c network defines how these functions create the calls and sessions.

3.2.4 Mobility Management Function

The mobility management function encompasses all of the functions that are required to support the mobility of the UE as it roams into and out of the coverage area of the IN-c device.

The mobility management function is comprised of a number of lower level functions that are required to manage the different aspects of mobility management that are needed between the IN-c device and the IN-c network.

3.2.4.1 Idle Mode Mobility Management Function

The idle mode mobility management function applies to both CS access mode of operation and the PS access mode of operation when a UE is not in an active call and the location of the UE changes to either within the coverage area of the IN-c device or as it moves out of the coverage area of the IN-c device. The idle mode mobility management function specifies the actions of the system when a UE does not have a connection active.

This function defines how the UE selects the IN-c device, for a UE that is permitted to access the IN-c network through the IN-c device. It also defines

how UEs that are either barred from accessing the IN-c device or barred from accessing the IN-c network.

3.2.4.2 Active Mode Mobility Management Function

The active mode mobility management function applies to both CS access mode of operation and the PS access mode of operation when a UE is active in a call and the location of the UE changes to either within the coverage area of the IN-c device or as it moves out of the coverage area of the IN-c device.

The function defines the handover procedure to manage the mobility as the location of the point of contact between the UE and the point of contact in the network changes.

3.2.5 Radio Resource Management Function

The radio resource management function controls the use of the radio resources. The radio resource management function is resident in both the IN-c device and the IN-c network.

3.2.5.1 IN-c Device Radio Resource Management Function

The IN-c device is responsible for controlling many aspects of the radio resources it uses. The device operates either within a set of known parameters that are previously defined by the IN-c network, or autonomously. The types of parameters that the IN-c device may control include items such as the cell scrambling code, the cell transmit power (within a range defined by the IN-c network), allocation of the spreading codes, admission control function.

3 2.5.2 IN-c Network Radio Resource Management Function

The IN-c network is responsible for defining limits and specific values for the radio resources that the IN-c device is able to utilise. Examples of the radio resources controlled by the IN-c network are the maximum and minimum powers that the IN-c device may use, the range of scrambling codes that the IN-c may use, the cell identity of the IN-c device, the location area and routing area codes assigned to the IN-c device and the UARFCN allocated for use by the IN-c device.

3.2.6 Network Management Function

The network management functions provide the facility to manage both the IN-c device and the IN-c network. The IN-c device contains a network management agent. Both SNMP [15] and TR69 [16] element control protocols are supported by the IN-c device.

Within the IN-c network, there is an Element Management System (EMS) that is responsible for configuring and customising both the IN-c devices as well as required entities within the IN-c network.

3.2.7 Billing and Charging Function

The billing and charging function is the mechanism through which the operator can assess the resources utilised by the subscriber and from that generate a bill for that subscriber.

The billing and charging function is implemented in both the IN-c device and also the IN-c network. The function requires the collection of a range of different CDRs that are passed to the billing and charging functions within the IN-c network.

3.2.8 Security Function

The security function provides a range of security mechanisms The security mechanisms include: authentication to ensure that the entities in the system are valid; ciphering to ensure that user data and signalling data can be kept confidential; copy protection to ensure that the IN-c device cannot be fraudulently manufactured; and hacker security to prevent unauthorised access to functions either in the IN-c device or the IN-c network.

3.2.9 Emergency Call Function

The emergency call function is the mechanism through which an emergency call can be made from a user registered on the IN-c device to an appropriate authority via the IN-c network.

3.2.10 QoS Function

The QoS function provides mechanisms by which the Quality of Service of the links between the IN-c device and the IN-c network can be established and controlled.

3.2.11 Software Download Function

The software download function provides a mechanism through which an upgrade to the software in the IN-c device can be achieved.

3.2.12 Lawful Intercept Functions

The lawful intercept function provides the mechanism by which calls and sessions between the UE and the elements in the IN-c network can be monitored from within the IN-c network.

3.2.13 Location Awareness Functions

The location awareness function is a mechanism through which the location of the IN-c device can be defined and used under certain circumstances.

3.2.14 Prevention of Roaming Fraud Functions

The prevention of roaming fraud function is the mechanism which can be utilised to prevent an IN-c device that should be deployed in one country /network being used to access that network from a different country and thereby obtaining service fraudulently.

3.3 Logical Architecture

The logical architecture for the IN-c network including the IN-c device and the UE is illustrated in Figure 2.

The network nodes required for the two variants of the architecture are highlighted. The first variant, referred to as the Pre-IMS architecture includes an MSC and GMSC entities The second variant of the architecture, referred to as the IMS-Ready architecture includes the minimum elements of the IMS required to support the operation of the IN-c devices.

3.3.1 UE

The UE is the User Equipment. This is the device that is used by the subscriber to access either the normal 3GPP macro network or the services provided by the IN-c device whilst connected to the IN-c network.

The IN-c device and network were designed to operate with standard 3GPP Release 99 UEs. Should the subscriber wish to utilise some of the services provided from later 3GPP specifications, such as HSDPA that is defined in the 3GPP Release 5 specifications, then the UE must be capable of supporting those services.

For UEs that are capable of operating in either 3GPP Release 99 mode of operation, or a 3GPP Release 6 IMS mode of operation, then the IN-c device and the IN-c network shall force the UE to operate in a 3GPP Release 99 mode and perform the necessary protocol conversion.

The interface between the UE and the IN-c device is the 3GPP Uu interface defined by the 3GPP Release 99 specifications [9].

3.3.2 IN-c Device

The IN-c device functions are an amalgamation of a number of 3GPP network elements. A block diagram of the logical nodes contained within the IN-c device is illustrated in Figure 3. The IN-c device comprises a Node B, RNC, MSC, SGSN, GGSN, P-CSCF, SIP-UA, MGCF and EAP agent

The IN-c device shall come in three classes. The different classes are intended to support different types of deployment. The expected type of deployments are defined in Table 1 below

IN-c Class	Typical Deployment
Class 1	Residential / SOHO
Class 2	Office, Shopping Mall,
Class 3	Stadiums, Halls,

Table 1 IN-c Classes and Typical Deployments

3.3.2.1 IN-c Internal Node B Functions

The IN-c device shall include the functions of the Node B. It shall comprise an RF transmitter and receiver that are capable of meeting the Local Area Cell Class specifications defined in the 3GPP Release 6 specifications [10].

In addition, it shall support the physical channels outlined in Table 2 below for the different classes of device.

Channel	Number of Channels Supported		
	Class 1	Class 2	Class 3
P-CPICH	1	1	1
SCH	1	1	1
P-CCPCH	1	1	1
S-CCPCH	1	2	4
DPDCH	3	10	30
DPCCH	3	10	30
PRACH	1	2	5
AICH	1	2	5
HS-SCCH	1	2	4
HS-PDSCH	5	10	15
HS-DPCCH	1	2	4

Table 2 IN-c Device Physical Channel Support

The Node-B function in the IN-c Device shall provide the following functions:

- UL open loop power control
- UL closed loop power control
- DL closed loop power control
- MAC-hs

The Node-B is responsible for the power control of the IN-c device within limits defined by the RRM function. The power setting function shall be dynamic and based on measurement made by the UEs.

3 3.2.2 IN-c Internal RNC Functions

The IN-c device includes the functions of the RNC. It shall provide support for the following RABs and SRBs:

RB/RAB	Number of RBs / RABs Supported		
	Class 1	Class 2	Class 3
SRB0 – UL	1	2	4
SRB0 – DL	1	2	4
SRB1, SRB2, SRB3	3	10	30
RAB (<64kb/s)	3	10	30
RAB (>64kb/s)	3	5	10
RAB – HS	2	5	10

Table 3 IN-c Device Support for Radio Bearers and Radio Access Bearers

The layer 2 protocols (MAC, RLC and PDCP) and the layer 3 protocols (RRC) shall all be terminated within the IN-c device.

The RNC functions supported shall include:

- Radio Resource Management
- Cell Power Setting
- Ciphering
- Mobility Management Control Functions

3 3.2.2 1 Radio Resource Management (RRM) Function

The IN-c device shall monitor and control the radio resources allocated at any instant in time. The resource management function includes the management of the channelisation code tree, the control of the power allocated per code and per user and admission control

The code tree that is used in the WCDMA standard is a finite resource, the RRM shall allocate codes from the tree based on current IN-c device loading and likely future requirements.

The power control management function ensures that each of the physical links to the connected UEs has sufficient power to retain the connection. The power control algorithms shall operate within the global power level settings defined by the cell power setting function.

The admission control function is responsible for gating each new user onto the IN-c device. The purpose of the admission control shall ensure that each user added to the IN-c device can be done so in a manner that satisfies their individual QoS, transmit power and backhaul bandwidth requirements.

3.3.2 2.2 Cell Power Setting

The cell power setting algorithm is a function that is traditionally not part of the Node B. The cell power setting utilises measurements made by one or more UEs of the surrounding macro and other IN-c device cells, which, together with an algorithm, define the maximum power levels that are allowed to be used by the IN-c device.

The operator, via the EMS management system, may specify absolute maximum cell power setting to safeguard any interference concerns in certain radio environments

3.3.2.2.3 Ciphering Function

This ciphering function in the IN-c device relates to the ciphering that exists across the radio interface between the UE and the IN-c device. The ciphering function in the IN-c device shall be responsible for selecting and controlling the ciphering algorithms, performing the ciphering procedures.

3.3.2.2.4 Mobility Management Control Function

The mobility management functions in the IN-c device relate specifically to handover Three different forms of handover are supported, idle mode handover, active mode handover and inter IN-c Device handover.

Idle mode handover defines the mechanism by which the handover between the IN-c device and a normal macro cell takes place, in either direction. The

mechanism is based on the cell reselection algorithms defined within the 3GPP specifications. Two approaches to the cell reselection shall be supported. In the first approach the IN-c device is part of the same PLMN as the macro cell, i.e. they have the same MCC and MNC. In the second approach the PLMN for the IN-c is different to that of the macro cell, but is defined as the HPLMN within the USIM in the UE used by the subscriber.

The support for active mode handover shall depend upon whether a pre-IMS network or an IMS-Ready network is being used in the IN-c network.

For the pre-IMS network, the active mode handover requires the movement of a connection from an MSC in the macro network to the SIP-IWF, or from the SIP-IWF to an MSC in the macro network. In either case, the originating MSC or SIP-IWF acts as the anchor MSC for the duration of the connection until the connection drops.

The handover from the macro network to the IN-c device is not currently supported. The management of the neighbour lists in the macro cell is an issue that will require careful planning as the IN-c devices are deployed. The handover from the IN-c device to the MSC is supported. The SIP-IWF acts as an anchor MSC for the duration of the handover. Details of the handover can be found in a later section.

Handover for the IMS-ready network shall be based on the VCC specifications defined by 3GPP[11].

3 3.2.3 IN-c Internal MSC Functions

The IN-c device shall include the functions of an MSC. The layer 3 protocols: MM, CC, SS, and SMS shall all be terminated in the MSC. The IN-c device shall receive MM service requests from the UE that is within the coverage area of the IN-c device The IN-c device shall validate that the UE is entitled to use the IN-c device and then authenticate the device with the IN-c network. After successfully registering, the UE shall establish a VoIP connection to the SIP-IWF for the pre-IMS network or the S-CSCF for the IMS-Ready network.

The MSC functions in the IN-device shall also include the support for supplementary services (SS) and the support for the 3GPP Short Message Service (SMS). The support for the SS is divided amongst the IN-c device and entities in the IN-c network.

The support of the SMS service shall be provided by the IN-c device. The MSC function in the IN-c device terminates all of the SMS requests for both MO and MT SMS. The SMS requests shall be converted to a SIP message by the SIP message function. The SIP message shall be forwarded to the SIP-IWF for the pre-IMS architecture or the S-CSCF for the IMS-ready architecture.

3.3.2.4 IN-c Internal SGSN Functions

The IN-c device shall include the functions of the SGSN. The layer 3 protocols GMM and SM shall be supported and terminated within the IN-c device. When a UE requests the establishment of a PDP context the requests come to the SGSN function in the IN-c device and shall be converted to IP data connections to the IN-c network.

Two operator configurable options for the packet data connections that the IN-c device can establish to the IN-c network shall be supported. The simplest is to allow a UE to access the IP data services directly from the IN-c device. This shall facilitate simple and low cost Internet access.

The alternative packet data connection option is to allow the UE to access the operator's specific data services that reside within the IN-c network To facilitate the access to the operator specific services the IN-c device shall use a secure tunnel to the operator's data network. The access function shall allow the use of an existing tunnel, or establish a child tunnel It shall be an operator configurable option as to which tunnel type shall be setup.

3.3.2.5 IN-c Internal GGSN Functions

The IN-c device shall include the functions of the GGSN. The GGSN is used when the connection to an external IP network is required. The GGSN will obtain an IP address from an external AAA server using DHCP.

3.3.2.6 IN-c Internal P-CSCF Functions

The IN-c device shall include the functions of the P-CSCF.

In the IMS-ready network, the P-CSCF shall act as specified in [6], except for the QoS control functions, which are not required due to the tight control of QoS and resources within the IN-c device.

For the Pre-IMS network the P-CSCF shall not be required. The functions of the SIP-UA will be sufficient to support the requirements for call and session control.

3.3.2.7 IN-c Internal SIP-UA Functions

The IN-c device includes the functions of a SIP User Agent. The SIP UA shall support two slightly different variants of SIP.

3.3.2.7.1 Pre-IMS Networks

For pre-IMS networks, the SIP-UA shall support the standard SIP functions defined in [7] and some of the extensions defined subsequently by the IETF. This implementation shall include the support for the UMTS AKA procedures.

The peer SIP entity for the SIP-UA in the IN-c device shall be the SIP-IWF The SIP-UA will register via the SIP-IWF and perform session establishments via the SIP-IWF.

3.3.2.7.2 IMS-Ready Networks

For the IMS-Ready networks, the SIP-UA shall support the SIP functions defined in [6]. A number of private SIP extensions are added to the SIP protocol for specific use within 3GPP IMS networks.

The SIP-UA shall have two peer entities in the IN-c network. The first peer entity shall be the S-CSCF which shall be responsible for registration with the IMS and the establishment of SIP sessions.

The second peer entity in the IN-c network shall be the SIP-IWF. The SIP-IWF is present in the IMS-Ready IN-c network to facilitate the extraction of the mobility information that is required as the UE roams into and out of the coverage of the IN-c device. In this context, the SIP-IWF shall act as a SIP-MAP gateway and is responsible for the extraction of mobility information such as the authentication vectors.

3.3.2.8 IN-c Internal IWF Functions

The IN-c IWF function shall be responsible for the conversion between the standard 3GPP CS and PS signalling protocols to an equivalent set of SIP based protocols. The specifics of the mapping are presented in detail in the call flows presented later in this specification.

3.3.2.9 IN-c Internal MGW Functions

The IN-c MGW function shall provide mechanisms for conversion between different media types.

The MGW function is intended for use when an IMS-Ready network is deployed to facilitate the conversion of a CS media stream into one or more PS streams.

Although explicit transcoding shall not be supported, the MGW shall support the conversion between the different transport protocols, in particular to convert a H.324M media stream multiplexed onto a CS synchronous bearer, into a number of RTP/UDP/IP streams that are suitable for transmission across the IN-c network. The IN-c device shall terminate the H.324M protocols.

3.3.2.10 IN-c Internal EAP/IKEv2 Agent functions

The IN-c device includes an EAP/IKEv2 agent function. The EAP/IKEv2 agent shall be responsible for the establishment of the IPSec tunnels between the IN-c network and the IN-c device.

The keying material for the IPSec tunnels between the IN-c device and the IN-c network shall be derived from the keys in the USIM that is present in the IN-c device.

3.3.2.11 IN-c Internal Management Agent

The IN-c device includes an internal management agent. The management agent shall support both SNMP [15] and TR69 [16] management protocols. The functions of the management agent shall be the configuration of the IN-c device, software download and alarms generation and reporting.

The configuration of the various parameters within the IN-c device shall be based on the information retrieved from the EMS. The configuration information is prestored in the EMS and may be downloaded on request from the IN-c device.

A software download function shall provide an update to all or part of the software that is resident in the IN-c device. The software download feature provides a mechanism through which new services and product features are installed on the IN-c device

3.3.2.12 IN-c Internal Local Database

The IN-c device shall include a local database. The local database shall be used:

To define the identity of the UEs that are allowed access via the IN-c device.

- To define the identity of the home phone number.
- To contain the keying information for UEs that are using the device.
- To store the configuration information received from the EMS
- To store the locally derived configuration parameters.

The local database shall have a backup copy in permanent memory and a working copy in RAM.

The identity information that is stored in the local database for the subscribers that are permitted to use the IN-c device shall include the IMSI, the IMEI of the terminal the subscriber uses and their MSISDN.

The detailed contents of the local database are defined in section 11.1.1.2.

3.3.2.13 IN-c Internal USIM

The IN-c device shall include a USIM. The USIM shall be used by the IN-c network to register and authenticate the IN-c device. The USIM shall include the key information that has a peer entity in the HLR/HSS. The key information in the USIM and the HSS are used as part of the authentication procedure and to generate the keys for the IPSec tunnels when they are established.

3.3.2 14 IN-c Internal API Agent

The IN-c device shall include an internal API agent. The API agent is used to facilitate the development of operators specific and third part services based on the features of the IN-c device. The API agent shall be based on the OSGi [17] initiative.

3.3.3 AAA Server

The AAA server is the Authentication, Authorisation and Accounting server that shall be responsible for a range of security related procedures. The AAA server may be based on either RADIUS [12] or DIAMETER [13] protocols.

The EAP agent in the IN-c device shall inter-work with the AAA server via the Wa interface [14]. The IN-c device shall obtain IN-c network entity address information from the AAA server

The WAG [14] and the TTG [14] shall inter-work with the AAA server to authenticate the IN-c device and then subsequently establish secure IPSec tunnels between the IN-c device and the TTG.

The HLR/HSS inter-works with the AAA server. The key information stored in the HLR/HSS shall be requested by the AAA server.

3.3.4 WAG

The WAG is the Wireless Access Gateway [14] that shall provide firewall functionality at the edge of the IN-c network. The WAG may exist as a separate entity, or may be part of the router and security gateway at the network edge.

3.3.5 TTG

The TTG is the Tunnel Termination Gateway [14] that shall provide secure IPSec tunnels to the IN-c device.

The TTG shall be linked to the IN-c device via the Wp / Wn interface and the AAA server via the Wm interface.

The TTG shall be responsible (with the AAA server) for authentication and authorisation of the IN-c device prior to the establishment of the first secure IPSec tunnel.

3.3.6 EMS

The EMS is the Element Management System. The EMS is the management entity in the IN-c network that shall be responsible for the configuration and management of the IN-c device and the SIP-IWF.

The EMS shall support both SNMP and TR69.

The EMS shall automatically configure on request an IN-c device after the IN-c device has been authenticated by the IN-c network.

The EMS shall download software updates to IN-c device when these updates become available and according to a schedule that is defined by the operator

3.3.7 WAP-GW

The WAP gateway shall provide access for the IN-c device to the operator specific services The WAP gateway does not require any specific enhancements to support the access from a UE attached to the IN-c device.

3.3.8 GGSN

The GGSN is the Gateway GPRS Support Node [18], it is the edge of the PS domain within the operators network.

Within the IN-c network the GGSN does not require any specific enhancements. The IN-c device shall interface with the GGSN in the operator's network when a UE attached to the IN-c device requires access to the operator specific services.

3.3.9 SGSN

The SGSN is the Serving GPRS Support Node [18], it is the PS domain interface between the UTRAN and the operator's core network.

Within the IN-c network the SGSN does not require any enhancements The SGSN shall be used in the IN-c network to retrieve authentication and SGSN context information which shall be passed to the IN-c device, or to pass authentication and SGSN context information to the IN-c device

The passing of the authentication and SGSN context information between the different network entities shall be an operator option and not a requirement for the operation of the system. If the IN-c had no access to the data stored in the SGSN, the IN-c device shall request the IMSI from the handset and retrieve the necessary information from the HLR/HSS

The IN-c device may retrieve or transmit authentication and SGSN context information to and from the SGSN via the SIP-IWF.

3.3.10 SIP-IWF

The structure of the SIP-IWF is illustrated in Figure 4.

The physical structure of the SIP-IWF is in no way constrained by the functional representation illustrated in Figure 4, and could be realised in a single or a number of physical modules.

3.3.10.1 Registrar

Within the SIP-IWF, there shall be a function called the SIP Registrar. The SIP registrar is only required for pre-IMS networks, and is optional for the IMS-Ready network

The Registrar is a database that shall store the identity and registered location for all of the UEs that are active on an IN-c device within the network.

For the pre-IMS network, the Registrar shall perform a dual role. It is responsible for the registration of the UE for the mobility management context that the UE is using as well as registering the UE for the SIP session that it is likely to establish.

For the IMS-Ready IN-c network, the Registrar shall only be required to register the MM contexts of the UEs. The SIP session registration is managed by the S-CSCF in the IMS.

3.3.10.2 MGCF

The MGCF is the Media Gateway Control Function within the SIP-IWF. The MGCF shall be responsible for translating the SIP session requests into the SS7/ISUP call establishment messages.

The details of the message conversion are presented in the later sections where the specific details of the message flows are presented.

3.3.10.3 MGW

The MGW is the media Gateway function within the SIP-IWF. The MGW is responsible for transcoding the AMR RTP media streams received from the

IN-c device into an appropriate format (e.g. G.711 PCM) for transmission over the SS7 network.

3.3.10.4 VLR

The VLR is the Visitor Location Register function within the SIP-IWF. The VLR functions within the SIP-IWF are not required to be as comprehensive as those defined for a VLR within the normal PLMN. The data that shall be stored in the VLR is the location of the UE and the authentication information for that UE.

The information that is required to be stored in defined in a later section of this document.

3.3.10.5 SIP-to-MAP Gateway

The SIP-to-MAP gateway shall be a function within the SIP-IWF that is used to exchange data between the SIP-IWF, the IN-c device and entities in the IN-c network such as the HLR, SGSN and MSC/VLR

The SIP-to-MAP gateway shall receive a request for data from the IN-c device (such as authentication vectors) and then retrieves the data from the appropriate network entity. The incoming request shall be in the form of a SIP REGISTER message which is directed towards the SIP-to-MAP gateway, the outgoing request shall be a MAP request for authentication parameters from the HLR/HSS.

The SIP-to-MAP gateway shall be used for a range of functions including:

- Exchange of authentication information
- Exchange of handover information
- Exchange of handover messages
- Exchange of SGSN context information
- Exchange of SMS messages between IN-c devices and SMSC

The details of the different messages exchanges are presented in later sections that address the specific message flow details.

3.3.10.6 MM Agent

The MM-Agent is the Mobility Management Agent function within the SIP-IWF. The MM Agent shall be responsible for managing the MM connections that exist in UEs that are no longer within the coverage area of the IN-c device.

The MM-Agent shall act as the "Anchor MSC" in terms of the signalling support that is required as a UE moves from the coverage area of the IN-c device into the coverage area of a cell connected to the macro network.

The MM-Agent is only required for the pre-IMS IN-c network. For the IMS-Ready network the handover function shall be managed through the use of a VCC [11].

The operation of the MM Agent is illustrated through the message flows that are presented in later sections

3.3.10.7 TDM and SS7 Interface Unit

The TDM and SS7 interface unit provides the physical and lower layer protocols for access to a TDM and SS7 based network within the SIP-IWF.

The physical interfaces are implementation dependent, but typically are multiple E1 trunks

The lower layer protocols may be MTP1-3 or may be based on M3UA for transport of MTP and higher later messages via an IP transport.

3.3.11 SMSC

The SMSC is the Short Message Service Centre within the IN-c network.

Within the IN-c network the SMSC does not require any enhancements from its likely implementation in the operator's normal macro network.

The SMSC may be used in both the pre-IMS and the IMS-Ready networks. The SMSC exchanges SMS data with the SIP-IWF using the MAP protocol.

3.3.12 HLR/HSS

The HLR / HSS are the Home Location Register / Home Subscriber Server within the IN-c network.

The HLR/HSS are required to support the security and service control functions that are required by the IN-c network. The HLR/HSS does not require any enhancements to support the services delivered by the IN-c device The interfaces to the HLR/HSS and the data requested from the HLR / HSS are the same as they are currently.

3.3.13 MSC/VLR

The MSC/VLR is the Mobile Switching Centre / Visitor Location Register.

The MSC/VLR is not directly used by the IN-c network, but shall be required in events such as handover or idle mode cell reselection where authentication information is required.

No changes are required to the MSC/VLR to support the operation of the IN-c device within the IN-c network.

3.3.14 GMSC

The GMSC is the Gateway Mobile Switching Centre The GMSC is the entry point into an operator's PLMN.

For the pre-IMS network, the GMSC is required within the IN-c network to define the location of the SIP-IWF that controls the IN-c device to which the UE is attached.

For the IMS-Ready network the incoming call requests are routed via the S-CSCF and do not require the services of the GMSC.

There are no changes required to the GMSC to support the operation of the IN-c device within the IN-c network.

3.3.15 S-CSCF

The S-CSCF is the Serving Call Session Control Function. Within the IMS-Ready network, this is one of the main SIP proxies.

The S-CSCF is used in the IMS-Ready network to register the UEs and perform service control.

There are no changes required to the S-CSCF to support the operation of the IN-c device within the IN-c network.

3.3.16 MGCF

The MGCF is the Media Gateway Control Function The MGCF controls the MGW within the IMS-Ready network.

The IN-c device does not have any logical connection to the MGCF except via the S-CSCF when sessions / calls are established.

There are no changes required to the MGCF to support the operation of the IN-c device within the IN-c network

3.3.17 MGW

The MGW is the Media Gateway. The MGW shall transcode and change the transport technology for the media streams within the IMS-Ready network.

The IN-c device does not have any logical connection to the MGW except via the S-CSCF when sessions / calls are established.

There are no changes required to the MGW to support the operation of the IN-c device within the IN-c network.

3.4 Assignment of Functions to General Logical Architecture

Function	UE	IN-c	WAG	SIP-IWF	TTG	AAA	SGSN	GGSN	HLR	MSC/VLR	S-CSCF	EMS
Access Control and Registration:												
IN-c Device: Access Control		X	X		X	X			X			
IN-c Device: UE Access Control	X	X										
IN-c Network: Registration	X	X		X			X		X	X		
Packet Routeing & Transfer.												
Internal Network Data Routing	X	X	X		X			X				
External Network Data Routing	X	X										X
NAT		X			X	X						
Tunnelling		X			X			X				
Compression		X			X							
Ciphering	X	X			X							
Call / Session Establishment	X	X		X	X						X	
Mobility Management.												
Idle Mode Mobility Management	X	X										X
Active Mode Mobility Management	X	X		X						X		
Radio Resource Management												
IN-c Device RR Management		X										X
IN-c Network RR Management												
Network Management		X		X								X
Billing and Charging		X		X				X				
Security	X	X		X	X				X		X	
Emergency Call	X	X		X								
QoS		X										
Software Download		X										X
Lawful Intercept		X		X	X							
Location Awareness		X							X			X
Prevention of Roaming Fraud		X		X								X

Table 4 Mapping of Functions to Logical Architecture

3.5 Control and User Planes

3.5.1 Control Plane

The control plane is a set of protocols that are defined to control specific aspects of the network. Different control protocols are used across the different interfaces. The control plane is intended to control a user data flow

between different entities. A control data flow between two entities could be carried as user plane data across an intervening interface.

3.5 1.1 UE – IN-c Device

The control plane between the UE and the IN-c device is based on a number of existing 3GPP protocols and is presented figuratively in Figure 5.

The protocols for the CS domain mode of operation and the PS domain mode of operation are both presented.

Legend:

- Call Control (CC): This protocol supports the establishment and disconnection of circuit switched services. The CC protocol is part of the CS domain suite of protocols and is defined in TS 24.008 [4].

- Session Management (SM): The SM protocol is responsible for the activation, deactivation and modification of PS data sessions referred to as PDP contexts. The SM protocol is part of the PS domain suite of protocols and is defined in TS 24.008 [4].

- Supplementary Services (SS): SS is responsible for the provision of supplementary services for the CS domain. SS is defined in TS 24.008 [4].

- Short Message Service (SMS). This protocol provides for the transfer of mobile originated and mobile terminated SMS messages across the radio interface to the IN-c device The SMS protocol is defined in TS 23.040 [19].

- Mobility Management (MM): The MM protocol handles the mobility management functions across the radio interface between the UE and the IN-c device. The MM functions that are supported include the registration and authentication functions, security, the establishment and control of MM signalling contexts for higher layer protocols, and location area updating. The MM protocol is part of the CS domain suite of protocols and is defined in TS 24.008 [8]

- GPRS Mobility Management (GMM): Similar to the MM protocol, but on the packet side, there is the GMM. GMM manages registration (attach), de-registration (detach), security including authentication, GMM signalling contexts and routing area updates. The GMM protocol is part of the PS domain suite of protocols that are defined in TS 24.008 [8].

- Radio Resource Control (RRC): RRC is responsible for establishing and controlling connections between the UE and the IN-c device. The connections take the form of radio bearers that are used for signalling (signalling radio bearers) or user plane data (radio access bearers). The RRC protocol also manages radio mobility functions such as handover and cell selection and reselection. The RRC protocol is defined in TS 25.331 [20].

- Radio Link Control (RLC): This protocol provides a range of different QoS defined links across the radio interface. There will be multiple RLC links between each UE and the IN-c device. The QoS of the link is defined by higher layers to meet the QoS required for the service or the signalling connection. The RLC protocol is defined in TS25.322 [22].

- Medium Access Control (MAC): The MAC provides resource scheduling and control for the different data flows that are required across the radio interface. The MAC is defined in TS 25.321 [22].

- Layer 1: This is also referred to as the physical layer. The physical layer implements what is commonly referred to as WCDMA. The functionality of the physical layer is described in a number of specifications, but summarised by TS 25.201 [24].

3.5.1.2 IN-c Device – SIP-IWF / S-CSCF – CS Services

The control plane protocols that are used between the IN-c device and the SIP-IWF for the pre-IMS network and the S-CSCF for the IMS-Ready network are considered in Figure 6.

Legend:

- Session Initiation Protocol (SIP): SIP is designed to control multimedia sessions over an IP network. SIP with some proprietary header extensions has been selected by 3GPP to control the 3GPP IMS-Ready network. The SIP-IWF used in the pre-IMS network does not use the extensions that are defined for the IMS and used in the IMS-Ready network. The SIP protocol is defined in RFC 3261 [31].

- Session Description Protocol (SDP): This protocol is used to define the type of media that is being requested for instance, for a session that is being created. The SDP protocol is defined in RFC 4566 [32].

- UDP is the User Datagram Protocol defined in RFC 768 [27].

- Remote IP is the "inner" IP address that exists between the IN-c device and the SIP-IWF. The IP address is allocated via the IN-c network as part of the tunnel establishment phase. The IP protocol conforms to RFC 791 [28].

- IP Security Encapsulating Security Payload (IPSec ESP): This is a subset of the IPSec family of security protocols. ESP provides a mechanism for encapsulating an IP packet within a second IP packet, encrypting the combined packet and adding a packet authentication header. The ESP protocol is defined by RFC 4303 [29].

- Transport IP is the outer IP address that is used to transport the encrypted payload to the TTG. The IP address for the outer IP packet is defined by the local service provider for the transport network that is used by the IN-c device.

- GPRS Tunnelling Protocol – User plane (GTP-U): This protocol is defined for use in the GPRS core network to tunnel IP datagrams between packet data nodes. The GTP-U defines a simple encapsulation protocol that is used to link the endpoints of the tunnel connections. The GTP-U is defined in TS 29.060 [30].

3.5.1.3 IN-c Device – SIP-IWF / GGSN – PS Services

Legend:

- GPRS Tunnelling Protocol – Control plane (GTP-C): This protocol is used to establish the PDP context tunnels from the TTG to the GGSN. The GTP-C is defined in TS 29.060 [30].

- IPSec / IKEv2: These are the protocols that are used to establish the IPSec tunnels from the IN-c device to the TTG. IPSec and IKEv2 are defined in RFC2401 and RFC 4306 [33, 34].

3.5.1.4 IN-c Device – EMS

The interface between the SIP-IWF and the EMS is used for the management and control of the SIP-IWF. The protocols used across that interface are illustrated in Figure 10.

Legend:

- Simple Network Management Protocol (SNMP): SNMP is the network management protocol selected to manage the SIP-IWF from the EMS. SNMP is defined in RFC 1157 [15].

3.5.1.5 IN-c Device – AAA Server

This interface is used as part of the IN-c authentication procedure.

Legend:

- RADIUS is a AAA protocol defined in RFC 2138 [12], and DIAMETER is an improved alternative protocol define in RFC 3588 [13].

3.5.1.6 SIP-IWF – EMS

The interface between the SIP-IWF and the EMS is used for the management and control of the SIP-IWF. The protocols used across that interface are illustrated in Figure 10.

3.5.1.7 SIP-IWF – HLR

The interface between the SIP-IWF and the HLR is used for extracting subscriber information from the HLR

3.5.1.8 SIP-IWF – MSC/VLR

The interface between the SIP-IWF and the MSC/VLR is used for the extraction of subscriber information such as the authentication vectors. It is also used as part of the handover procedure from the SIP-IWF to the MSC-VLR. The interface protocols are illustrated in Figure 12.

3.5.1.9 SIP-IWF – SGSN

The interface between the SIP-IWF and the SGSN is used as part of the routing area update procedure. The information that is passed between the SIP-IWF and the SGSN is the SGSN context information that will include the state of any active PDP contexts as well as the subscriber data such as authentication vectors. The interface between the SIP-IWF and the SGSN is illustrated in Figure 13.

3.5.2 User Plane

3.5.2.1 UE – IN-c Device – CS Services

The user plane is a set of protocols that are defined to facilitate the transfer of user information between peer entities in the network. The user plane protocols may also include some control elements to ensure the flow of user plane information (e.g error management procedures and flow control)

3.5.2.2 IN-c Device – SIP-IWF / MGW – CS Services

The user plane between the IN-c device and the SIP-IWF for the pre-IMS network and between the IN-c device and the MGW for the IMS-Ready network is illustrated in Figure 14.

Legend:

- Payload: This is the media payload that carries the CS media A number of different media payload formats are defined. To support the AMR and W-AMR voice codecs an RTP payload format has been defined in RFC 3267 [25].
- Real Time Protocol: RTP is used to transport the real time media payloads such as audio and video. RTP defines a frame format, synchronisation, timing information and a control protocol. The RTP protocol is defined in RFC 3550 [26].

3.5.2.3 IN-c Device – SIP-IWF / GGSN – PS Services

The user plane between the IN-c device and the GGSN / App server is illustrated in Figure 15.

4. Access Control and Registration

Access control shall be divided into three functions: the IN-c device access control; the IN-c device UE access control; and the IN-c network registration.

The IN-c device access control shall ensure that only valid and authorised IN-c devices may access the IN-c network. To control access a USIM shall be included within the IN-c device. The cryptographic functionality of the USIM and peer functionality in the HSS in the network shall be used to authenticate the IN-c device.

The IN-c device UE access control shall limit the access of UEs to the IN-c device to those that have been registered for use. The IN-c device shall contain a subscriber database that defines the IMSI and IMEI of the UEs that are entitled to gain access to the IN-c network via the IN-c device. The subscriber database may be populated manually by the user, or automatically via the EMS. The choice of whether user controlled access or user controlled access shall be defined by the operator and passed to the IN-c device via the configuration information.

The IN-c network registration function shall limit access to the IN-c network to those UEs that the operator permits. Using the USIM in the UE, the operator may allow or deny access based on the subscriber's identity defined through the IMSI

4.1 IN-c Device: Access Control

The IN-c network shall support access control functions. The network access control functions are required to ensure that the IN-c device that is requesting access to the IN-c network is a valid device. A USIM shall be included in the IN-c device. The IN-c network shall authenticate the USIM and hence the IN-c device.

The procedure to authenticate the IN-c device is illustrated in Figure 16 below.

The IN-c device will never be in a roaming scenario, only the use of the Wa interface illustrated in Figure and defined in TS 23.234 [14] for the extraction of security parameters from the AAA server shall be considered The IN-c device shall support both the RADIUS and the DIAMETER implementation of the Wa interface .

The Wx interface between the AAA server and the HSS shall be based on the DIAMETER protocol. The use of proprietary protocols based on RADIUS is not defined within this specification, but is not excluded from use. The protocol operation across the Wx interface is defined in TS 23.234 and TS 29 234 [14, 35].

The following message sequences consider the IN-c device authentication and authorisation. In the first case shown in Figure 16 the RADIUS protocol is used across the Wa interface The example shown is for the case when the EAP-AKA [38] authentication protocol is used.

1) The IN-c device shall request authentication from the IN-c network by sending a RADIUS Access-Request message that includes the EAP Response/Identity message. The EAP identity is defined as the IMSI and is

included in the message. The use of the EAP protocol over RADIUS is defined by RFC 3579 [36].

2) The AAA server shall request a number of authentication vectors from the HSS. The IMSI for the IN-c device to be authenticated is contained within the request. The request is sent over the Wx interface using the DIAMETER Multimedia Authentication Request (MAR) message. The authentication vectors are based either on those defined by 3GPP for USIM authentication (EAP-AKA authentication), or on the GSM authentication triplet (EAP-SIM) with added message authentication.

3) The HSS responds to the AAA server with a set of authentication vectors in the DIAMETER Multimedia Authentication Answer (MAA) message. The additional authentication vectors are stored in the AAA server for future use. The AAA server may support either EAP-SIM [37]or EAP-AKA [38]. The case shown in the figure is for the EAP-AKA protocol.

4) The AAA server shall send a RADIUS Access-Challenge that includes a random number RAND and a Message Authentication code (MAC) in the case of the EAP-SIM and a RAND, MAC and authentication token (AUTN) in the case of the EAP-AKA. The IN-c device will recognise authentication protocol used.

5) For the EAP-AKA the IN-c device shall respond with a RADIUS Access-Request that includes the response (RES) and a MAC. The RES is derived by the USIM from secret keying information and the RAND.

6) The AAA server shall request the service profile for the IN-c device from the HSS using the DIAMETER Server Assignment Request (SAR) message. The service profile will allow the AAA server to verify that the IN-c device is allowed to access the IN-c network.

7) The HSS responds with the subscriber service profile for the IN-c device in a DIAMETER Server Assignment Answer (SAA) message.

8) The AAA server shall decide whether the IN-c device is allowed access to the IN-c network In this instance the IN-c device is allowed access.

9) The AAA server shall indicate to the IN-c device that the authentication and authorisation procedure was successful via a RADIUS Access-Accept message that contains the EAP-Success packet.

In the second case shown in Figure 17 the DIAMETER protocol is used across the Wa interface.

1) The IN-c device shall request authentication from the IN-c network by sending the DIAMETER EAP-Request message defined in RFC 4072 [39]. The request includes the EAP Response/Identity message. The EAP identity is defined as the IMSI and is included in the message

2) The AAA server shall request a number of authentication vectors from the HSS using the DIAMETER MAR message. The IMSI for the IN-c device to be authenticated is contained within the request. The request is sent over the Wx interface using the DIAMETER protocol. The authentication vectors are based either on those defined by 3GPP for USIM authentication (EAP-AKA authentication), or on the GSM authentication triplet (EAP-SIM) with added message authentication.

3) The HSS responds to the AAA server with a set of authentication vectors in the DIAMETER MAA message. The additional authentication vectors are stored in the AAA server for future use The AAA server may support either EAP-SIM [37] or EAP-AKA [38] The case shown in the figure is for the EAP-AKA protocol.

4) The AAA server shall send the DIAMETER EAP-Answer message that encapsulates the EAP-Request/AKA-Challenge message. This message shall include a random number RAND and a Message Authentication code (MAC) in the case of the EAP-SIM and a RAND, MAC and authentication token (AUTN)

in the case of the EAP-AKA The IN-c device will know the authentication protocol used from the message contents

5) For the EAP-AKA the IN-c device shall respond with DIAMETER-EAP-Request encapsulating an EAP-Response/AKA-Challenge message. The message shall include a response (RES) and a MAC. The RES shall be derived by the USIM from secret keying information and the RAND.

6) The AAA server shall request the service profile for the IN-c device from the HSS using the DIAMETR SAR message. The service profile will allow the AAA server to verify that the IN-c device is allowed to access the IN-c network.

7) The HSS responds with the subscriber service profile for the IN-c device using the DIAMETER SAA message.

8) The AAA server shall decide whether the IN-c device is allowed access to the IN-c network. In this instance the IN-c device is allowed access.

9) The AAA server shall indicate to the IN-c device that the authentication and authorisation procedure was successful using the DIAMETER-EAP-Answer message that encapsulates the EAP-Success message.

4.2 IN-c Device: UE Access Control

The IN-c device shall provide a UE access control function. The UE access control within the IN-c device ensures that only UEs that are allowed to utilise the IN-c device may gain access. The access control shall use the IMEI of the UE and the IMSI that is stored in the USIM of the UE.

The access control data (IMSI and IMEI) shall be stored in the local database that is present in the IN-c device for authorised subscribers. The main index into this local database shall be the IMSI of the subscriber that is allowed access. In addition, single or multiple IMEIs may be associated with the permitted IMSI.

To illustrate the access control within the IN-c device two scenarios are considered. In the first scenario the UE accesses the IN-c device with a UE in which the IMSI and the IMEI are both stored in the subscriber database. In the second scenario a UE accesses the IN-c device, but the IMEI is not known, but the IMSI is known.

In both of these scenarios the interactions with the IN-c network are not shown. Here we are only interested in the local access gating functions within the IN-c device, and not the IN-c network gating functions. The IN-c network gating functions are considered later It is assumed that the that the IMSI of the UE is known and stored in the subscriber database, and a valid set of authentication information is available for that IMSI.

The scenarios considered here are for the use of location area updates. The IN-c device shall also support IN-c UE access control based on routing area updates. It shall be an operator configurable option as to the type of update method and also the reject cause in cases where the access request fails. The two options are outlined in more detail in section 5.1 on idle mode mobility. The IN-c device shall store the operator preference in the local database.

4.2.1 IN-c Access Control – IMEI Known

1) The UE comes into the coverage area of the IN-c device and attempts to register using the Location Update Request. The UE will use the TMSI that was allocated in a previous registration as its identity.

2) The IN-c device shall request the IMEI of the UE using the Identity Request message. The IMEI shall be used as the first gating mechanism for the UE.

3) The UE responds with the Identity Response message that contains its IMEI.

4) The IN-c device shall check all of the registered IMSIs in the local database to see if the IMEI of the UE is associated with any of the IMSIs If the

IMEI is known and hence the IMSI, the authentication information (authentication vectors) for the UE can be retrieved from the local database in the IN-c device.

5) The IN-c device shall authenticate the UE by sending the Authentication Request message that shall include the RAND and AUTN parameters from the authentication vector.

6) The UE authenticates the IN-c device and computes a response from the RAND, AUTN and a secret key. The UE returns the response (RES) to the IN-c device using the Authentication Response message.

7) The IN-c device shall check that the RES is the same as the XRES in the local database. If it is the same, the UE is authentic and the location updating procedure may continue. The IN-c device shall send the Location Updating Accept message to the UE indicating the update was successful The message shall include a new TMSI and LAI obtained from the IN-c network (not shown).

8) The UE completes the procedure by sending a TMSI Reallocation Complete message to the IN-c device. The UE has been successfully authenticated and may now proceed to obtain various types of services from the IN-c network

4.2.2 IN-c Access Control – IMEI Not Known

In this scenario, the IMEI of the UE is not known in the IN-c device, but the IMSI of the subscriber is.

1) The UE comes into the coverage area of the IN-c device and attempts to register using the Location Updating Request message. The UE will use the TMSI that was allocated in a previous registration as its identity.

2) The IN-c device shall request the IMEI of the UE using the Identity Request message. The IMEI shall be used as the first gating mechanism for the UE.

3) The UE responds with its IMEI using the Identity Response message.

4) The IN-c device shall check all of the registered IMSIs in the local database to see if the IMEI of the UE is associated with any of the IMSIs. In this scenario, the IMEI is not found in the database

5) The IN-c device shall request the IMSI of the UE using the Identity Request message.

6) The UE responds with its IMSI contained in an Identity Response.

7) The IN-c device shall check to see if the IMSI of the UE is available in the local database. In this scenario it is and the UE is granted access. The IN-c device shall add the IMEI to the list of IMEIs that are associated with that IMSI within the local database The authentication information for the UE is retrieved.

8) The IN-c device shall authenticate the UE by sending the Authentication Request message that includes the RAND and AUTN parameters.

9) The UE authenticates the IN-c device and computes a response from the RAND, AUTN and a secret key. The UE returns the response (RES) to the IN-c device via the Authentication Response message.

10) The IN-c device shall check that the RES is the same as the XRES in the subscriber database. If it is the same, the UE is authentic and the location updating procedure may continue. The IN-c device shall send the Location Updating Accept message to the UE indicating the update was successful. The message will include a new TMSI and LAI.

11) The UE completes the procedure by sending a TMSI Reallocation Complete message to the IN-c device. The UE has been successfully authenticated and may now proceed to obtain various types of services from the IN-c network.

4.2.3 IN-c Access Control – IMSI Not Known

In this scenario a UE that is not registered in the subscriber database in the IN-c device attempts to perform a location update to the IN-c device.

The location update request shall be rejected with a cause. The cause is defined by the parameter UE_ACCESS_REJECT_TYPE1 that shall be stored in the local database and configured via the EMS. An example reject cause may be cause 13 "Roaming not allowed in this location area"

1) The UE comes into the coverage area of the IN-c device and attempts to register using the Location Updating Request message. The UE will use the TMSI that was allocated in a previous registration as its identity.

2) The IN-c device shall request the IMEI of the UE using the Identity Request message. The IMEI will be used as the first gating mechanism for the UE.

3) The UE responds with its IMEI carried in the Identity Response message.

4) The IN-c device shall check all of the registered IMSIs in the subscriber database to see if the IMEI of the UE is associated with any of the IMSIs. In this scenario, the IMEI is not found in the database.

5) The IN-c device shall request the IMSI of the UE using the Identity Request message.

6) The UE responds with its IMSI in the Identity Response message

7) The IN-c device shall check to see if the IMSI of the UE is present in the local database. In this scenario it is not. The IN-c device shall reject the access attempt being made by the UE.

8) The IN-c device shall send the UE a Location Updating Reject message. The contents of the message shall include a cause value. The cause value shall be taken from the parameter UE_ACCESS_REJECT_TYPE1 which is obtained from the local database.

4.3 IN-c Network: Registration

4.3.1 General Issues

The IN-c network registration function performs authentication and authorisation of the access attempts of UEs via the IN-c device. The registration functionality will differ slightly between the pre-IMS network and the IMS-Ready network.

For a pre-IMS network, the registration functions described in sub-section 4.3.2 shall be performed to ensure that the UE is both authentic and authorised to access the services of the IN-c network.

For an IMS-Ready network, the registration functions described in sub-section 4.3.2 are optional and may be performed based on a specific operator's requirement. For the IMS-Ready network the UE shall register with the IMS irrespective of whether the UE has registered with the SIP-IWF. The IMS registration procedures are defined in section 4.3.3

A configuration parameter SIP-IWF-REGISTER is used to define whether registration to the SIP-IWF is required in the IMS-ready case.

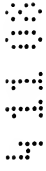
4.3.2 Registration with the SIP-IWF

The access authentication shall be based on the 3GPP cryptographic keys and algorithms stored on the USIM that is located within the UE and peered to the authentication centre located within the HLR/HSS. These procedures are defined in TS 33.102 [40].

The access authorisation is an access policy decision which is made using information for the subscription status of the subscriber that is stored in the HLR/HSS. In this version of the specification, the subscription status will consist of a flag that defines whether a specific UE is allowed to access the IN-c network or whether it is not allowed to access the IN-c network.

The authentication and authorisation functions may occur every occasion the UE performs a registration procedure (location area update or routing area update) to the IN-c device

The registration procedure occurs whenever a UE moves into the coverage area of the IN-c device. The registration procedure shall apply to the CS domain and the PS domain. The registration procedure is sub-divided into an initial registration attempt, a subsequent registration attempts and a periodic registration.



The initial registration attempt is referred to as IMSI Attach for the CS domain and GPRS Attach for the PS domain.

The subsequent registration procedures are the location area update for the CS domain and the routing area update for the PS domain.

The periodic registration is referred to as a periodic location area update for the CS domain and periodic routing area update for the PS domain.

All of the registration procedures outlined above are defined within the 3GPP specification TS 24.008 [4].

The following sub-sections considers the message flows for various registration scenarios The registration procedures for the Circuit Switched (CS) domain are considered first. The registration procedures for the Packet Switched (PS) domain follow.

4.3.2.1 CS Registration Using TMSI – UE Enters Coverage of IN-c Device

A number of scenarios are considered in which the UE was previously in the macro-network, has moved into the coverage area of the IN-c device and uses the TMSI allocated by the macro network to identify itself for the registration procedure.

The UE has been provisioned previously to use the IN-c device and consequently the IN-c UE access control is passed. The IN-c device has previously registered and been authenticated by the core network, and a secure signalling tunnel has been established.

4.3.2.1.1 TMSI and LAI Not Known by SIP-IWF

In this scenario the entity in the macro network that allocated the TMSI can not be identified. The SIP-IWF has to request authentication information from the HLR.

1) UE is activated while in the coverage area of the IN-c device. The UE performs the location area updating procedure including the TMSI and LAI allocated previously by the macro network The UE sends the Location Updating Request message to the IN-c device.

2) If the IN-c device can't locate the entity in the macro network where the TMSI was allocated, the IN-c device shall request the IMEI of the UE using the procedures described in section 4.2 and from the local database locate the IMSI.

3) The IN-c device shall send the SIP REGISTER request to the SIP-IWF. The IMSI is included in the form of the UE's private identity. The structure for the private identity is defined in the chapter 8 The initial REGISTER message shall not contain any cryptographic material or algorithms.

4) If the SIP-IWF does not have any valid authentication vectors for the UE, the HLR shall be requested to provide a set for the IMSI to be registered

In this case, the SIP-IWF shall send the MAP Send Identification request message including the IMSI as a parameter.

5) The authentication centre in the HLR generates a set of authentication vectors and returns them to the SIP-IWF in the MAP Send Identification Acknowledge message. The SIP-IWF shall store the vectors in its local database.

6) The SIP-IWF shall respond to the IN-c device with the SIP 401 Unauthorised response. The response shall include the authentication vectors.

7) The IN-c device shall start to authenticate the UE by sending the Authentication Request message. The message shall include the RAND and AUTN parts of the authentication vectors.

8) The USIM within the UE will authenticate the IN-c network and then compute a cryptographic response to the authentication request (RES). The UE sends the RES to the IN-c device in the Authentication Response message.

9) The IN-c device shall send a second SIP REGISTER request message to the SIP-IWF. The REGISTER request shall include the IMSI, RAND, AUTN and RES. The SIP-IWF shall compare the RES received from the IN-c device with the XRES received in the authentication vectors from the HLR. If the RES and the XRES match, the UE is deemed authentic and the registration may proceed.

10) The SIP-IWF shall notify the HLR that the UE has changed its registered location using the MAP Update Location message.

11) The HLR sends the service profile of the subscriber to the SIP-IWF via the MAP Insert Subscriber Data message. The service profile shall include whether the UE is entitled to use the services of the IN-c device. The SIP-IWF shall store the service profile in its local database.

12) The SIP-IWF shall acknowledge the receipt of the service profile to the HLR with a MAP Insert Subscriber Data Ack message.

13) The HLR acknowledges the updating of the location of the UE with the MAP Update Location Ack message.

14) If the UE is entitled to use the IN-c device the SIP-IWF shall allocate a TMSI and a LAI for the UE and respond with a SIP 200 OK response indicating that the location updating was successful. The 200 OK shall include the TMSI, LAI and an expiry timer that defines the length of time the registration is valid before a subsequent "periodic" update is required. The SIP-IWF shall store the TMSI and LAI in its local database.

15) The IN-c device shall store the TMSI and LAI in the local database linked to the IMSI. The TMSI/LAI shall be used by the IN-c device to detect subsequent location update attempts by that UE. The TMSI and the LAI shall be sent to the UE in the Location Area Updating Accept message.

16) The UE acknowledges the receipt of the new TMSI with the TMSI Reallocation Complete message.

4 3.2.1 2 TMSI and LAI Known by SIP-IWF

In this scenario the entity in the macro network that allocated the TMSI can be identified. The SIP-IWF requests authentication information from the MSC/VLR.

1) UE is activated while in the coverage area of the IN-c device. The UE performs the location area updating procedure including the TMSI and LAI allocated previously by the macro network by sending a Location Updating Request message.

2) If the IN-c device can't locate the entity in the macro network where the TMSI was allocated, the IN-c device shall request the IMEI of the UE using the

procedures described in section 4.2 and from the local database locate the IMSI.

3) The IN-c device shall send the SIP REGISTER request to the SIP-IWF. The message shall include the TMSI and the LAI obtained from the UE as the private identity to be registered. The structure for the private identity is defined in the chapter 8. The initial REGISTER message shall not contain any cryptographic material or algorithms.

4) From the LAI the PLMN-ID and LAC shall be extracted by the SIP-IWF. From the PLMN-ID and the LAC, the SIP-IWF shall identify the MSC/VLR that allocated the TMSI/LAI. The SIP-IWF shall request the identification information (IMSI) and any remaining, unused, authentication vectors from the MSC/VLR using the MAP Send Identification message.

5) The MSC VLR responds with the IMSI and any remaining authentication vectors using the MAP Send Identification Ack message. The SIP-IWF shall store the vectors in its local database.

6) The SIP-IWF shall respond to the REGISTER message from the IN-c device with the SIP 401 Unauthorised response. The response shall include the TMSI/LAI and one of the authentication vectors received from the MSC/VLR.

7) The IN-c device shall authenticate the UE by sending an Authentication Request message that includes the RAND and the AUTN from the authentication vector.

8) The UE authenticates the IN-c network and computes a response (RES) which it sends in a Authentication Response to the IN-c device

9) The IN-c device shall send a second SIP REGISTER request The REGISTER request shall include the IMSI, RAND, AUTN and RES. The message shall be sent to the SIP-IWF

10) On receipt of the second REGISTER message, the SIP-IWF shall compare the RES with the XRES obtained from the authentication vector. If they agree, it is a valid UE and the registration procedure can continue. The SIP-IWF shall inform the HLR the new location for the UE using the MAP Update Location message.

11) The HLR sends the service profile of the subscriber to the SIP-IWF using the MAP Insert Subscriber Data message. The service profile shall include whether the UE is entitled to use the services of the IN-c device.

12) The SIP-IWF shall acknowledge the receipt of the service profile to the HLR with the MAP Insert Subscriber Data Ack message. The SIP-IWF shall store the service profile in its local database.

13) The HLR cancels the location of the UE in the previous MSC/VLR with the MAP Cancel Location message.

14) The MSC/VLR acknowledges the location update for the UE with the MAP Cancel Location Ack message.

15) The HLR acknowledges the updating of the location of the UE by sending the MAP Update Location Ack message to the SIP-IWF

16) If the UE is entitled to use the IN-c device the SIP-IWF shall respond to the IN-c device with a SIP 200 OK response indicating that the location updating was successful. The 200 OK shall include a new TMSI/LAI and an expiry timer that defines the length of time the registration is valid before a subsequent "periodic" update is required. The SIP-IWF shall store the TMSI/LAI in its local database.

17) The IN-c device shall store the TMSI and LAI in the local database linked to the IMSI. The TMSI/LAI shall be used by the IN-c device to detect subsequent location update attempts by that UE. The TMSI and the LAI shall be sent to the UE in the Location Area Updating Accept message.

18) The UE acknowledges the receipt of the new TMSI with the TMSI Reallocation Complete message.

4.3.2.2 CS Registration Using TMSI – UE Still in Coverage of IN-c Device

In this scenario, the UE is activated whilst in the coverage are of the IN-c device where it was located when it was de-activated previously. The TMSI was allocated by the SIP-IWF, but the period of the registration has expired.

The authentication information in the SIP-IWF was previously obtained from an entity in the macro network. The message flows are illustrated in Figure 23

1) The UE is activated within the coverage area of the IN-c device. The UE performs a location update to the IN-c device using the Location Updating Request message.

2) In this scenario, the IN-c device shall identify the TMSI as one previously active. From the TMSI, the IN-c device shall identify the IMSI by searching the local database.

3) The IN-c device shall send the SIP REGISTER request with the IMSI of the UE defined as the private identity.

4) In this scenario, the SIP-IWF shall identify that the UE was previously registered with the SIP-IWF and still has a valid authentication vector for the UE. The SIP 401 Unauthorised response shall be sent to the IN-c device. The response shall include the RAND and AUTN from the authentication vectors that are stored in the SIP-IWF.

5) The IN-c device shall send an Authentication Request message to the UE. The authentication request shall include a RAND and an AUTN.

6) The UE authenticates the IN-c network. The UE then computes a response and sends this to the IN-c device using the Authentication Response message.

7) The IN-c device shall send to the SIP-IWF a second SIP REGISTER request which includes the IMSI, RAND, AUTN and RES.

8) The SIP-IWF shall compare the RES from the SIP REGISTER request with the XRES from the authentication vector. If the two agree, the UE is deemed authentic and the SIP-IWF proceeds to register the UE A TMSI/LAI shall be allocated to the UE and returned to the IN-c device using the SIP 200 OK response.

9) The IN-c device shall store the TMSI/LAI in the local database in the IN-c device. The IN-c device shall notify the UE that the registration attempt was successful and send the new TMSI/LAI to the UE using the Location Updating Accept message.

10) The UE acknowledges the receipt of the TMSI/LAI with the TMSI Reallocation Complete, and the registration procedure is completed.

4.3.2.3 CS Periodic Location Update

This scenario considers the periodic update registration functions. The UE will perform a periodic update as normal . The IN-c will translate this into a registration attempt to the SIP-IWF. The message flow is illustrated in Figure 24.

1) The periodic location area update timer in the UE expires. The UE performs a periodic location update. The UE will include the TMSI and the LAI in the Location Updating Request that it sends to the IN-c device.

2) The IN-c device receives the update request. The IN-c device shall check the local database to see if the TMSI is defined as being active. From the database the previously used authentication vector shall be retrieved

3) The IN-c device shall send a SIP REGISTER request to the SIP-IWF including the IMSI, RAND, AUTN and RES. The SIP-IWF shall compare the RES with the XRES that is stored with the authentication vector. The two

agree and so the SIP-IWF updates the expiry timer for the UE registration within its local database

4) The SIP 200 OK response shall be returned to the IN-c device. The response shall include the updated registration expiry timer. The response shall also include the new TMSI/LAI being allocated to the IN-c device. The SIP-IWF shall store the TMSI/LAI in its local database.

5) The IN-c device shall send the Location Updating Accept message to the UE. The message shall include the TMSI/LAI allocated by the SIP-IWF.

6) The UE acknowledges the receipt of the new TMSI/LAI with the TMSI Reallocation Complete message.

4.3.2.4 CS Periodic Location Update Fail

This scenario considers the case when the periodic location area update fails, possibly due to the UE moving out of coverage In this scenario the absence of the periodic update triggers a de-register event with the SIP-IWF The message flow is illustrated in Figure 25.

1) The IN-c device periodic update timer for a specific UE expires, but no update was received. The IN-c device shall detach the UE

2) The IN-c device shall sends a SIP REGISTER request message for the UE to the SIP-IWF. The expiry timer shall be set to 0 indicating that the UE shall be de-registered.

3) The SIP-IWF shall acknowledge the receipt of the Detach request by sending a SIP 200 OK response

4.3.2.5 PS Routing Area Update Using IMSI – UE Moved Domain

A packet switched routing area update is considered in Figure 26. The UE was previously in the IN-c network and has come into the coverage area of the

macro network. The UE identifies itself through the use of the TMSI that was allocated by the IN-c network.

1) The UE after selecting a cell in the new routing area will perform a routing area update. The Routing Area Update Request will be sent to the new SGSN.

2) The SGSN will request the SGSN context from the SIP-IWF which is identified by the RAI as the previous location for the UE

3) The SIP-IWF shall request some of the context information from the IN-c device and de-register the UE by sending a SIP REGISTER request to the IN-c device with the expiry timer set to zero.

4) The IN-c device shall respond to the SIP-IWF with the SGSN context information. The information returned by the IN-c device will be carried in a container that is passed to the SIP-IWF in the SIP 200 OK response. The container shall be carried in the body part of the SIP response with the format for the container defined in [1].

5) The SIP-IWF shall respond to the SGSN with the GTP SGSN Context Response. The response shall include the SGSN context information that was retrieved from the IN-c device as well as the required information stored in the local database in the SIP-IWF.

6) The GTP SGSN Context Acknowledge message is sent from the SGSN to the SIP-IWF indicating that the context was received correctly.

7) The SGSN notifies the HLR that the UE has moved to a new SGSN by sending a MAP Update Location message.

8) The HLR transfers the subscriber profile to the SGSN in the MAP Insert Subscriber Data message

9) The SGSN acknowledges the receipt of the subscription profile with the MAP Insert Subscriber Data Ack message

10) The HLR notifies the SIP-IWF that the UE has moved by sending the MAP Cancel Location message.

11) The SIP-IWF shall acknowledge the notification from the HLR with the MAP Cancel Location Ack message. The SIP-IWF shall update its local database to reflect the in-active status of the UE.

12) The HLR indicates to the SGSN that the location change is completed successfully with the MAP Update Location Ack message.

13) The SGSN indicates to the UE that the routing area update was successful and provides a new P-TMSI/RAI via the Routing Area Update Accept message.

14) The UE acknowledges the completion of the procedure with the Routing Area Update Complete message.

4.3.2.6 PS Periodic Routing Area Update – No PDP Context Active

A periodic routing area update is considered in Figure 27. The UE has been previously active within the IN-c, but a timer has expired and the UE will perform an update. In this scenario, there is no active PDP context.

1) The UE establishes a radio connection to the IN-c device.

2) To be deleted

3) To be deleted

4) A timer in the UE expires indicating that a periodic update is required. The UE sends a Routing Area Update Request indicating that the update type is a periodic update and contains the P-TMSI and RAI.

5) The IN-c device shall send a SIP REGISTER request to the SIP-IWF. The SIP REGISTER request shall include the IMSI, RAND, AUTN and RES used previously.

6) On receipt of the SIP REGISTER request, the SIP-IWF shall compare the RES with the XRES If they are both the same, the registration attempt shall proceed. A SIP 200 OK response shall be created. The response shall include a P-TMSI, RAI and a new value for the registration expiry timer. The SIP 200 OK response shall be sent to the IN-c device. The SIP-IWF shall store the value for the expiry timer in the local database.

7) On receipt of the SIP 200 OK response, the IN-c device shall send a Routing Area Update Accept message to the UE. The IN-c device shall store the P-TMSI, RAI and timer value in the local database linked to the IMSI of the UE.

8) The UE acknowledges the receipt of the update request with a Routing Area Update Complete message sent to the IN-c device.

4.3.2.7 PS Periodic Routing Area Update – PDP Context Active

A periodic routing area update is considered in Figure 28. The UE has been previously active within the IN-c device, but a timer has expired and the UE will perform an update. In this scenario, there is an active PDP context.

1) The periodic update timer has expired and the UE needs to perform a routing area update. The UE has an active PDP context; no radio connection is required to be established. The UE sends a Routing Area Update Request message to the IN-c device. The message contains the P-TMSI/RAI allocated previously.

2) The IN-c device shall check its local database to verify the UE is currently active The IN-c device shall update the registration period for the

UE. The SIP REGISTER request including the IMSI, RAND, AUTN and RES shall be sent to the SIP-IWF.

3) The SIP-IWF shall acknowledge a successful registration and send a SIP 200 OK response. The response shall include a new P-TMSI, RAI and expiry timer value. The SIP-IWF shall store the P-TMSI, RAI and timer in the local database.

4) The IN-c device shall store the P-TMSI, RAI and expiry timer in the local database. Then it shall send a Routing Area Update Accept to the UE indicating that the procedure was successful, and including the P-TMSI and RAI.

5) The UE acknowledges the completion of the procedure with the Routing Area Update Complete message.

4.3.3 Registration with the IMS

The registration to the IMS shall be performed by the IN-c device if the network is an IMS-Ready network. The registration procedure will be towards the S-CSCF whose identity is defined by the configuration information the IN-c device received from the EMS.

The IMS registration shall occur after the optional SIP-IWF registration procedure. Two scenarios are considered in this sub-section.

In the first scenario we assume that a registration to the SIP-IWF is not required and has not been performed, and in the second scenario we assume that a registration to the SIP-IWF is required and has been performed.

4.3.3.1 Registration to IMS – No SIP-IWF Registration

In this scenario, the UE has not registered with the SIP-IWF and is not required to register with the SIP-IWF. The IN-c device requires the IMSI of the UE. The IMSI for the UE can be identified if the IMEI of the UE is retrieved.

1) The UE moves into the coverage area of the IN-c device and initiates a registration procedure. The TMSI and LAI that were allocated by the macro network are passed to the IN-c device in the Location Updating Request message.

2) In this scenario, the IN-c device does not recognise the TMSI and the UE has not registered previously with the SIP-IWF. The IN-c device shall request the IMEI from the UE. The IMEI for the UE shall be converted into the IMSI for the UE using the local database in the IN-c device.

3) The IN-c device shall send a SIP REGISTER request to the S-CSCF in the IMS. The request shall include the IMSI in the form of the private identity for the UE. The identity of the S-CSCF is provisioned when the IN-c device is configured.

4) The S-CSCF does not have information on the UE. The S-CSCF will request a set of authentication vectors from the HSS. The Diameter MAR message is used to retrieve the vectors.

5) The HSS responds with a set of authentication vectors. The set of authentication vectors are returned using the DIAMETER MAA message.

6) The S-CSCF responds to the IN-c device with a SIP 401 Unauthorised response. The IN-c device shall be configured to appear as a P-CSCF and consequently the authentication vectors are returned to the IN-c device in the 401 response The IN-c device shall store the contents of the authentication vectors in the local database with a link to the IMSI of the UE.

7) The IN-c device shall send an Authentication Request message to the UE. The message shall include the RAND and AUTN parameters from the authentication vector stored in the local database.

8) The UE authenticates the IN-c network, generates the response RES and puts it into an Authentication Response message which is sent to the IN-c device

9) The IN-c device shall create a second SIP REGISTER request message to be sent the S-CSCF that shall include the IMSI, RAND, AUTN and RES.

10) The S-CSCF verifies that the received RES and XRES from the authentication vector are the same. The S-CSCF then requests, from the HSS, the service profile for the UE using the DIAMETER SAR message.

11) The HSS responds to the S-CSCF with the service profile for the UE. The response is sent in the DIAMETER SAA message.

12) The S-CSCF sends the SIP 200 OK to the IN-c device indicating that the registration was successful. The S-CSCF also sends associated public identities to the IN-c device that indicate which other addresses have been registered for the UE. The IN-c device shall store the additional identities that are assigned to the UE in the local database.

13) The IN-c device shall respond to the UE with a Location Updating Accept message. The IN-c device will allocate a TMSI/LAI for the UE and include it in the message. The IN-c device shall store the TMSI/LAI in the local database linked to the IMSI of the UE.

14) The UE responds with the TMSI Reallocation Complete message indicating that the registration procedure is complete.

4.3.3.2 Registration to IMS – Previous SIP-IWF Registration

In this scenario, the UE has registered with the SIP-IWF. The IN-c device knows the IMSI and TMSI of the UE and that a registration attempt to the IMS is required

The IN-c device shall not authenticate the UE as it was authenticated when the access to the SIP-IWF was performed.

1) The IN-c device shall perform a registration to the S-CSCF once the registration to the SIP-IWF is complete. The IMSI/TMSI is known by the IN-c device.

2) The IN-c device shall send a SIP REGISTER request to the S-CSCF in the IMS. The request shall include the IMSI in the form of the private identity for the UE as defined for use in the IMS in TS 23.003 [3]. The identity of the S-CSCF is provisioned when the IN-c device is configured.

3) The S-CSCF does not have information on the UE. The S-CSCF will request a set of authentication vectors from the HSS. The Diameter command MAR is used to retrieve the vectors.

4) The HSS responds with a set of authentication vectors. The set of authentication vectors are returned using the DIAMETER MAA message.

5) The S-CSCF responds to the IN-c device with a SIP 401 unauthorised response The IN-c device shall be configured to appear as a P-CSCF; the authentication vectors are returned to the IN-c device. The IN-c device shall store the authentication vectors in the local database.

6) The IN-c device shall send an Authentication Request message to the UE. The authentication request message shall include the RAND and AUTN parameters from the authentication vector.

7) The UE authenticates the IN-c network and generates a response to the authentication request. The response RES is passed to the IN-c device in the Authentication Response message.

8) The IN-c device shall perform a second registration attempt to the UE. The SIP REGISTER request is sent to the S-CSCF. The request shall include the IMSI, RAND, AUTN and RES.

9) The S-CSCF verifies that the received RES and XRES from the authentication vector are the same. The S-CSCF then requests, from the HSS, the service profile for the UE using the DIAMETER SAR message.

10) The HSS responds to the S-CSCF with the service profile for the UE. The response is sent in the DIAMETER SAA message.

11) The S-CSCF sends the SIP 200 OK response to the IN-c device indicating that the registration was successful. The S-CSCF also sends associated public identities to the IN-c device that indicate which other addresses have been registered for the UE. The IN-c device shall store the additional identities that are assigned to the UE in the local database.

5. Mobility Management

5.1 Idle Mode

The Idle mode mobility management functions relate to the procedures by which the UE selects the IN-c device when it comes into its coverage area.

Two basic methodologies are defined. The choice on which methodology to employ is defined by a parameter IDLE_MODE_SELECT_TYPE. The operator shall choose between these two types be configuring this parameter in the IN-c device via the EMS.

The first method for idle mode mobility management shall use a different PLMN identity for the home PLMN (HPLMN as defined on the USIM). By defining the IN-c device PLMN identity as the home PLMN, the UE will naturally select that when it returns to the coverage area of the IN-c device.

In the second method, the same PLMN identity shall be used for the macro network and the IN-c network . The IN-c network shall be allocated some of the address space used by the macro network for the Location Area Identifiers (LAI). Additionally, an individual Routing Area Identifier shall be used to identify each IN-c device.

5.1.1 Different HPLMN IN-c Network and Macro Network

In this method the IN-c network shall be allocated a separate PLMN-Id to the PLMN-Id used by the macro network. The PLMN-Id shall be registered on the USIM as the Home PLMN (HPLMN) and as such has the highest priority. Additionally, on the USIM, the home network search timer shall be set to its minimum value, which is currently 6.

In this method the LAIs shall be allocated pseudo-randomly within a geographic area to each IN-c device. With 65,536 LAIs available, a large number of IN-c devices can be allocated before the number space is exhausted.

There are three scenarios that we need to consider here:

- UE authorised to use this IN-c device enters coverage area
- UE authorised to use a different IN-c device (USIM HPLMN same as IN-c network PLMN-Id) enters the coverage area.
- UE not authorised to use any IN-c device (USIM HPLMN same as the macro network PLMN-Id)

In addition to the procedure that defines the authorisation of the UE onto the IN-c cell, there is also an alternative method of attracting the UEs to the HPLMN using a gateway cell broadcast from the IN-c device. This procedure is described in detail in section 5.1.1.4 below.

5.1.1.1 UE Authorised on IN-c Device

When the UE arrives home, and the home search timer is triggered, the UE will locate the IN-c device as the PLMN-Id shall be set to the HPLMN of the UE.

The UE performs a location area update, the IMSI is obtained (either directly or in-directly – see 4.2). The location area update is successful and the UE camps on the cell provided by the IN-c device

5.1.1.2 UE Not Authorised on IN-c Device but with Same HPLMN

When the UE arrives in the coverage area of the IN-c device, and the home search timer is triggered, the UE will locate the IN-c device with the PLMN-Id set to the HPLMN of the UE.

The UE performs a location area update, the IMSI is obtained (either directly or in-directly - see 4 2). The IN-c device identifies that the UE is not registered and rejects the location update with the cause value defined by the parameter UE_ACCESS_REJECT_TYPE1 defined by the EMS as part of the IN-c configuration. The UE will then search for another cell and return to the cell on the macro network

5.1.1.3 UE Not Authorised on IN-c Device but with Different HPLMN

In this scenario the UE will not have the IN-c device broadcast PLMN-Id defined in its USIM as the HPLMN. The UE would only select the IN-c device as the "suitable cell" if all of the cells on the macro network were not suitable cells. In this case, the UE would be rejected in a manner similar to the case above. The UE will return to the macro network when a suitable cell on the macro network is located.

5.1.1.4 Gateway Cell to Attract UEs to the HPLMN

To facilitate fast idle mode handover some variants of the IN-c device are capable of broadcasting a second cell on the same frequency. This second cell will be referred to here as a gateway cell. The gateway cell acts as an attractor for any handset entering the IN-c coverage zone and is designed to direct the handset towards the IN-c primary cell

In this mode the IN-c broadcasts a PLMN on its primary cell that is different to the PLMN of the macro network. The gateway cell broadcasts a PLMN that is identical to that of the macro network. The gateway cell consists of the

minimum channels required to cause the handset to generate a connection request and to send to the handset a connection reject.

In this configuration the system information of the gateway cell includes the IN-c primary cell in its neighbour list. The scrambling code of the gateway cell is chosen to be in the neighbour list of the local macro cell. The PLMN of the IN-c primary cell is configured to be an equivalent PLMN of the HPLMN of the handset.

When a handset enters the coverage zone of the IN-c device it sees the gateway cell as a valid handover candidate of the macro network and generates a connection request towards the gateway cell. If the handset is allowed to access the IN-c primary cell the IN-c device will respond with a connection reject with a redirection information element that will cause the handset to retry the IN-c primary cell as an equivalent PLMN The handset can also be rejected at this stage if required by sending a connection reject.

Once directed toward the IN-c primary cell the handset will perform a location update procedure and the IN-c device will either accept or reject this based upon the standard access control procedure for the IN-c device.

Handsets will perform this procedure when the IN-c gateway cell is received at a signal level that triggers the standard idle mode handover procedure. If a handset is not allowed to use the IN-c device due to access restrictions the handset will be rejected and will fall back to using the macro cell as the next best candidate cell. If a handset is allowed to use the IN-c device it will be location update accepted onto the IN-c primary cell as an equivalent PLMN to the HPLMN The local macro cell is configured to be in the neighbour list of the IN-c primary cell so when the handset leaves the IN-c coverage zone the handset will perform a standard idle mode handover back to the macro network.

This technique has the advantage of causing the idle mode handover both into the IN-c and out of the IN-c to take place very quickly with handset decisions being made at the paging cycle measurement rate.

5.1.2 Same HPLMN IN-c Network and Macro Network

This method shall require a percentage of the operator's macro network location area address space be reserved for use by the IN-c network. As an example if we assume 25% of the address space can be used, this creates 16,384 LAIs for use in the IN-c network.

For the definition of the RAI, for each LAI there is an 8 bit RAC, leading to 256 RACs per LAI. If the each of the LAIs is sub-divided into 256 RACs, there would be 4,194,304 unique RAIs within the network.

The presence of the Gs interface shall be broadcast by the IN-c device, all UEs attempting to access the IN-c device shall perform a combined LAU and RAU whenever the RAI changes.

The methodology is illustrated in the following three scenarios set out below.

- A UE returns to its home IN-c device and is authorised to use this IN-c device
- A UE enters the coverage area of the IN-c device, is authorised on a different IN-c device, but is not allowed access to the IN-c network via this device.
- The UE enters the coverage area of the IN-c device, it is not authorised to use the IN-c network on any IN-c device

To differentiate between the last two scenarios, the IN-c device would need to proceed with all registration attempts to the point where the IN-c network defines whether the UE is a valid UE or not, rather than allowing the IN-c device to gate un-registered users.

The benefit of letting the IN-c network perform the gating is that the subsequent routing area update attempts by UEs not registered to access the

IN-c device can be reduced by barring the LAI. The penalty of this approach is that all registration attempts will require access to the IN-c network.

5.1.2.1 UE Returning to Home IN-c Device

On returning to the coverage area of the IN-c device, the UE, through its idle mode cell selection procedures will find the cell. The signal level and quality for the IN-c device should be better than for the macro network, the PLMN identity is the same, but the routing area identifier is different. The UE will perform a routing area update to the IN-c device.

The UE is registered to use the IN-c device and consequently the scenarios in 4.2 1 for the success case will apply and the routing area update will be successful. The UE will camp on the cell provided by the IN-c device.

5.1.2.2 UE Attempting Access on to IN-c Device - Allowed on IN-c Network

A UE that is not registered to use this IN-c device will select the cell through its idle mode cell selection procedures. The UE will attempt a routing area update to the cell, but shall be rejected with the cause defined by the parameter UE_ACCESS_REJECT_TYPE2 that is configured by the EMS. This scenario is similar to the reject scenario presented in 4.2.3. After receiving this rejection cause, the UE will look for an alternative cell and attempt a routing area update, or a location area update to that cell

To facilitate some signalling benefits outlined in the following scenario, the IN-c device could validate the entitlement of the UE to access the IN-c network through any IN-c device, before deciding to reject on this UE.

5.1 2.3 UE Attempting Access to IN-c Device - Not Allowed on IN-c Network

A UE that is not registered to use any IN-c device will select the cell through its idle mode cell selection procedures The UE will attempt a routing area update to the cell, but will not be successful as the IMSI in the UE is not registered in the IN-c database

As an operator configured option, the IN-c device can proceed with the registration attempt to the IN-c network to the point where the HLR defines that the UE is not permitted to use the IN-c network.

In the case when the UE is prevented from using the IN-c network, the UE could be rejected with the cause set to the value defined by the parameter UE_ACCESS_REJECT_TYPE1 that is configured by the EMS. The benefit of this is that it will prevent the UE from accessing similar IN-c devices in the neighbourhood.

5.2 Active Mode

Active mode mobility management refers specifically to handover between the IN-c device and the cells in the macro network. At present this handover is only intended for the Pre-IMS network case The IMS-Ready handover is based on the Voice Call Continuity (VCC) standardisation being pursued within the 3GPP standards bodies.

The details of VCC will be added in a later release of this document when the standardisation effort within 3GPP is further progressed.

There are two types of handover that we may consider. Handover from the macro cell to the IN-c device and handover from the IN-c device to the macro cell. This version of the document only considers the handover between the IN-c device and the macro cell. The handover in the opposite direction is feasible in terms of signalling, but does present problems to the operator in terms of neighbour cell list management. This is particularly an issue in urban environments where there may be several hundred IN-c devices within the coverage area of a macro cell.

5.2.1 CS Handover IN-c Device to Macro Network

The handover from the IN-c device to a cell in the macro network shall be managed in a manner similar to an inter-MSC handover in the macro network. The MAP signalling shall be inter-worked with SIP signalling within the SIP-IWF.

The handover procedure for a successful handover from the IN-c device to a cell in the macro network is illustrated in Figure 31.

1) The UE has established a call to some destination terminal via the SIP-IWF and the IN-c device. The UE has started to move out of the coverage area of the IN-c device.

2) The UE shall be requested to send measurements reports when certain signal related criteria have been met. The measurement report shall contain a list of measurements from the IN-c device, and the strongest neighbour macro cells.

3) On receiving the measurement reports from the UE, and other measurements made by the IN-c device, the IN-c device shall decide that a handover to the macro network is required to maintain the continuity of the call. To initiate the handover the IN-c device shall send a SIP REFER request to the SIP-IWF. The SIP REFER request shall contain a proprietary SIP header (P-Relocation-Information). This header shall contain the SRNS Context information from the IN-c device that shall be passed to the RNC in the macro network to ensure the continuity of the call.

4) The SIP-IWF shall receive the SIP REFER request containing the P-Relocation-Information and shall know that this is part of a handover procedure The SIP-IWF shall prepare a MAP Prepare-Handover-Request message. This message shall include the SRNS-Context received from the IN-c device The message shall be sent to the MSC that has been identified as the recipient of the handover call.

5) The identity of the RNC to be used for the handover is identified within the P-Relocation-Information The MSC sends the RANAP Relocation Request message to this RNC The information within this message is sufficient for the RNC to establish the necessary channels in preparation for the handover from the UE

6) When the RNC within the RNS has established the channels necessary for the UE, the RNC sends the RANAP Relocation Request ACK to the MSC. This indicates that the handover may go-ahead, and includes necessary information such as allocated channel identifies.

7) The MSC sends the MAP Prepare-Handover-Response to the SIP-IWF. This message indicates to the SIP-IWF that the handover is proceeding.

8) The SIP-IWF shall send the SIP 202 Accepted response to the IN-c device. The 202 Accepted response indicates to the IN-c device that the handover request has been accepted and the handover may continue. The response shall include the proprietary header P-Relocation-Information, but the SIP-IWF shall add some additional fields to provide necessary information such as the channel identity to be used on the new cell.

9) The IN-c device shall send the Physical Channel Reconfiguration message to the UE. This message informs the UE that the physical channel that the UE is currently using shall change The physical channel reconfiguration message shall provide all of the information that is necessary for the UE to establish the connection to the new cell.

10) When the UE has synchronised with the new cell attached to the RNC, the UE will send a Physical Channel Reconfiguration Complete message. This message indicates that the UE has acquired the new cell and that the physical layer aspects of the handover are complete.

11) When the RNS detects the presence of the UE on the new cell, it sends the RANAP Relocation Detect message to the MSC.

12) The MSC sends the MAP Process Access Signal Request message to the SIP-IWF. This indicates that UE has been detected on the new cell.

13) The SIP-IWF shall send a SIP NOTIFY message to the IN-c device. The NOTIFY message shall inform the IN-c device of an event. In this case the event is the completion of the handover to the MSC.

14) The IN-c device shall acknowledge the NOTIFY message with the SIP 200 OK response.

15) When the connection of the UE to the RNC is complete, the RNC sends a RANAP Relocation Complete message to the MSC.

16) On receipt of the Relocation Complete message, the MSC sends, to the SIP-IWF, the Send-End-Signal-Request preparing the MSC for the termination of the MM and CC connection when the call is completed.

17) The SIP-IWF shall send the SIP BYE request to the IN-c device to close the session in the IN-c device.

18) The IN-c device shall acknowledge the receipt of the BYE request by sending a 200 OK response back to the SIP-IWF.

19) The call continues in the network. The SIP-IWF shall act as the anchor MSC during the duration of the call. Any MM, CC, SS or SMS requests shall be managed by the SIP-IWF until the call is completed. At the point the call completes the new MSC will become the serving MSC for that UE.

20) The call completes and the resources used by the UE are relinquished.

21) The SIP-IWF shall send the MAP Send-End-Signal-Response when the call is completed This indicates to the new MSC that the call is over. The UE can now perform a location update to the new MSC.

6. Commissioning

6.1 Initial Installation

Two methods for the initial installation shall be supported. The first method shall require the subscriber to enter the IMSIs of the UEs that are entitled to access the IN-c device and the IN-c network. The second method shall require the EMS to configure the IMSIs that are entitled to access the IN-c device and the IN-c network. A parameter UE_ACCESS_CONTROL that is configured by the EMS.

The procedures deployed for a manual activation are outlined in Figure 32. This procedure will be followed by the first (master) user, but can also be followed to permit subsequent users to access the network.

The network configured access control procedure is outlined in Figure 33.

7. Security Aspects

There are a number of security issues and requirements that need to be addressed for the IN-c to CN interface.

7.1 HBS Authentication and Initial Tunnel Establishment

The IN-c device requires a secure connection to the IN-c network to permit the downloading of new software, configuration information and signalling messages. This section describes how this initial secure tunnel is established.

7.1.1 Tunnel Establishment - Radius Based TTG & EAP-SIM

This section assumes the EAP-AKA authentication procedures There are equivalent procedures based on the EAP-SIM.

1) The IN-c device shall initiate the establishment of a secure tunnel by sending the IKE-SA-INIT Request message to the TTG. The message shall include the Security Parameter Index (SPI) in the header (Hdr), the Security Association (SA) payload that defines the cryptographic algorithms supported

by the IN-c device, the Diffie-Hellman (D-H) value and a Nonce defined by the IN-c device

2) The TTG shall respond with an IKE-SA-INIT Response message that includes its SPI, its choice of cryptographic algorithms from the list provided by the IN-c device and included in the SA, a D-H value and a Nonce. This message completes the Diffie Hellman exchange required to compute the parameter SKEYSEED [34]. All subsequent exchanges, except for the headers shall be encrypted and integrity protected.

3) The IN-c device shall proceed with the establishment of the first child Security Association (CHILD_SA) by sending the IKE-AUTH Request message which includes Hdrs that contains the SPI, the IMSI to identify the IN-c device, the configuration payload parameter (CFG_REQ) that indicates that a remote IP address is required, a set of SAs for the CHILD_SA that is being established, a Traffic Selector (TS) that is used to filter packets (set to a wide range in this message) and an APN that shall be used to define the end network address. The IKE-AUTH message shall initiate an authentication procedure as part of the tunnel establishment. The absence of an AUTH parameter in the IKE_AUTH message indicates that EAP is being selected for authentication [34].

4) On receipt of the IKE-AUTH Request message, the TTG shall send the RADIUS Access-Request message that is carrying an empty EAP message. This message shall define the identity (the IMSI of the IN-c device in this case) of the entity to be authenticated. The message shall be sent to the AAA server.

5) The AAA server shall respond with the EAP-Request/SIM Start message defined by RFC 4186 [37]. The Start packet is a sub-type of the EAP-SIM type The Start packet shall contain a list of EAP-SIM versions supported by the AAA server. This response is sent in the RADIUS Access-Challenge message.

6) The TTG shall forward the EAP-Request/SIM Start message to the IN-c device using the IKE-AUTH Response message. This message (except for the header) shall be ciphered and integrity protected based on the keying material derived in the earlier part of the IKE exchange.

7) The IN-c device shall respond to the EAP-Request/SIM Start message with an EAP-Response/SIM Start packet. The response message shall include a random number (Nonce) and the selected version from the received list.

8) The TTG shall forward the EAP-Request/SIM Start message to the AAA server using the RADIUS Access-Request message.

9) The AAA server, on receipt of the EAP-Response/SIM Start message shall request a set of authentication triplets from the HSS by sending the Diameter Multimedia-Authentication-Request (MAR) message. The message shall include the IMSI to authenticate and the number of triplets requested.

10) The HSS computes the set of authentication triplets for the specified IMSI and returns them in the Diameter-Multimedia-Authentication-Answer message.

11) The AAA server shall continue in the authentication procedure by sending a RADIUS Access-Challenge message that contains the EAP-Request/SIM-Challenge to the TTG. The parameters to this message shall include a random number, RAND, and a Message Authentication Code (MAC). The MAC shall be derived from the message and it there to validate the message integrity when received by the IN-c device.

12) The TTG shall send the EAP-Request/SIM-Challenge payload to the IN-c device encapsulated within an IKE-AUTH Response message. Additional message contents include the Hdrs field that defines the SPIs (un-ciphered), the identity of the TTG, a certificate verifying the keys used by the AAA server, and AUTH the authentication payload used to integrity protect the message and based on the shared secret key.

13) The IN-c device shall validate the received message by checking AUTH matches a locally derived value. It shall then extract the contents of the EAP-Request/AKA-Challenge message (RAND and MAC). From these parameters the IN-c device shall authenticate the message from the AAA server and compute a response MAC. The MAC derived by the IN-c device shall be sent to the TTG within an IKE-AUTH Request message that carries an EAP-Response/SIM-Challenge message.

14) The TTG shall extract the EAP-Response/SIM-Challenge payload (including MAC) from the message from the IN-c device and shall put it into a RADIUS Access-Request message. The message shall be sent to the AAA server.

15) The AAA server shall check that the MAC received matches the MAC derived locally.

16) If the two MACs match, the AAA server shall send a RADIUS Access-Accept message that carries the EAP-Success message to the TTG. The contents of the EAP-Success message shall also include the derived keying material obtained during the authentication procedure.

17) In the next stage, the TTG shall obtain authorisation for the IN-c device to create a tunnel to an end-point identified by an APN (IN-c APN in this example). The TTG shall send a RADIUS Access-Request message that initiates the authorisation procedure.

18) The AAA server shall send a Diameter-Server-Assignment-Request (SAR) message to the HSS. The SAR message shall request the HSS to supply the AAA server with the service profile for the IN-c device identified by the IMSI of the device that is a parameter to the message.

19) The HSS returns to the AAA server the IN-c device service profile in the Diameter-Server-Assignment-Answer (SAA) message. The contents of the message are the requested service profile.

20) The AAA server shall verify that the IN-c device has the required permissions to access the IN-c network based on the service profile received.

21) The AAA server shall confirm that the IN-c device is authorised to use the IN-c network by sending the RADIUS Access-Accept message that includes the IMSI of the IN-c device as a parameter.

22) On receipt of the Radius Access-Accept message, the TTG shall compute the AUTH parameter for the first and second IKE-SA-INIT messages. These two messages were sent without integrity protection, and so the derived keys (now known by IN-c device and TTG) shall be used to generate this authentication parameter.

23) The TTG shall pass the EAP-Success message to the IN-c device indicating that the authentication and authorisation were successful.

24) The IN-c device shall send the AUTH parameter to the TTG. The AUTH parameter shall be derived from the first IKE-SA-INIT message and the MSK. The TTG shall compare this AUTH parameter with the one derived locally

25) The TTG shall send the AUTH parameter it derived for the second IKE-SA-INIT message. This shall be used by the IN-c device to check that the second message was an authentic message. The IKE-AUTH Response message shall also includes a CFG_REPLY that includes the assigned Remote IP address, the Security Associations and the selected Traffic Selectors (TS)

7.1.2 Tunnel Establishment - Diameter Based TTG & AKA-SIM

This section assumes the EAP-AKA authentication procedures. There are equivalent procedures based on the EAP-SIM.

1) The IN-c device shall initiates the establishment of a secure tunnel by sending the IKE-SA-INIT Request message to the TTG. The message shall include the Security Parameter Index (SPI) in the header (Hdr), the Security Association (SA) payload that defines the cryptographic algorithms supported by the IN-c device, The Diffie-Hellman (D-H) value and a Nonce defined by the IN-c device.

2) The TTG shall respond with an IKE-SA-INIT Response message that includes its SPI, its choice of cryptographic algorithms from the list provided by the IN-c device and included in the SA, a D-H value and a Nonce. This message completes the Diffie Hellman exchange required to compute the parameter SKEYSEED [34]. All subsequent exchanges, except for the headers shall be encrypted and integrity protected.

3) The IN-c device shall proceed with the establishment of the first child Security Association (CHILD_SA) by sending the IKE-AUTH Request message which includes Hdrs that contains the SPI, the IMSI to identify the IN-c device, the configuration payload parameter (CFG_REQ) that indicates that a remote IP address is required, a set of SAs for the CHILD_SA that is being established, a Traffic Selector (TS) that is used to filter packets (set to a wide range in this message) and an APN that can be used to define the end network address. The IKE-AUTH message shall initiate an authentication procedure as part of the tunnel establishment. The absence of an AUTH parameter in the IKE_AUTH message shall indicate that EAP is being selected for authentication [34].

4) On receipt of the IKE-AUTH Request message, the TTG shall send the Diameter EAP Request message that is carrying a null EAP message. This message shall define the identity (the IMSI of the IN-c device in this case) of the entity to be authenticated The message is sent to the AAA server.

5) The AAA server, on receipt of the EAP-Request/Identity message shall request a set of authentication vectors from the HSS by sending the Diameter

Multimedia-Authentication-Request (MAR) message. The message shall include the IMSI to authenticate and the number of vectors requested

6) The HSS computes the set of authentication vectors for the specified IMSI and returns them in the Diameter-Multimedia-Authentication-Answer message.

7) The AAA server shall continue in the authentication procedure by sending a Diameter-EAP-Answer message that contains the EAP-Request/AKA-Challenge. The parameters to this message shall include a random number RAND, and authentication token (AUTN) and a Message Authentication Code (MAC).

8) The TTG shall send the EAP-Request/AKA-Challenge payload to the IN-c device encapsulated within an IKE-AUTH Response message. Additional message contents shall include the Hdrs field that defines the SPIs (un-ciphered), the identity of the TTG, a certificate verifying the keys used by the AAA server, and AUTH the authentication payload used to integrity protect the message and based on the shared secret key

9) The IN-c device shall validate the received message by checking AUTH matches a locally derived value. It shall then extract the contents of the EAP-Request/AKA-Challenge message (RAND, AUTN and MAC). From these parameters the IN-c device shall authenticate the AAA server and compute a response RES. The RES shall be sent to the TTG within an IKE-AUTH Request message that carries an EAP-Response/AKA-Challenge message.

10) The TTG shall extract the EAP-Response/AKA-Challenge payload (including RES) from the message from the IN-c device and puts it into a Diameter-EAP-Request message. The message shall be sent to the AAA server.

11) The AAA server shall check that the RES received matches the XRES from the authentication vector.

12) If the RES and the XRES match, the AAA server shall send a Diameter-EAP-Answer message that carries the EAP-Success message. The contents of the EAP-Success message shall also include the Master Session Key (MSK) that was derived during the authentication procedure.

13) In the next stage, the TTG shall obtain authorisation for the IN-c device to create a tunnel to an end-point identified by an APN (IN-c APN in this example). The TTG shall send a Diameter-AA-Request message [42] that initiates the authorisation procedure.

14) The AAA server shall send a Diameter-Server-Assignment-Request (SAR) message to the HSS. The SAR message shall request the HSS to supply the AAA server with the service profile for the IN-c device identified by the IMSI of the device that is a parameter to the message.

15) The HSS returns to the AAA server the IN-c device service profile in the Diameter-Server-Assignment-Answer (SAA) message. The contents of the message are the requested service profile.

16) The AAA server shall verify that the IN-c device has the required permissions to access the IN-c network based on the service profile received.

17) The AAA server shall confirm that the IN-c device is authorised to use the IN-c network by sending the Diameter-AA-Answer message that includes the IMSI of the IN-c device as a parameter

18) On receipt of the Diameter-AA-Answer message, the TTG shall compute the AUTH parameter for the first and second IKE-SA-INIT messages. These two messages were sent without integrity protection, and so the MSK (now known by IN-c device and TTG) shall be used to generate this authentication parameter

19) The TTG shall pass the EAP-Success message to the IN-c device indicating that the authentication and authorisation were successful.

20) The IN-c device shall send the AUTH parameter to the TTG. The AUTH parameter shall be derived from the first IKE-SA-INIT message and the MSK. The TTG shall compare this AUTH parameter with the one derived locally.

21) The TTG shall send the AUTH parameter it derived for the second IKE-SA-INIT message. This shall be used by the IN-c device to check that the second message was an authentic message. The IKE-AUTH Response message shall also includes a CFG_REPLY that includes the assigned Remote IP address, the Security Associations and the selected Traffic Selectors (TS).

8. UE Addressing and Identification to SIP-IWF

The addressing mechanism used to identify the UEs to the SIP-IWF is based on the identifiers defined for the IMS, but with some extensions. This structure for the identifiers used by the IN-c device when identifying UEs to the SIP-IWF is presented here.

For the SIP messaging to the SIP-IWF, there shall be two types of UE identification information used, both based on the 3GPP IMS identifiers [3]. The first identifier is referred to as a public identity (sip or tel URI) and the second a private identity in the form of a NAI

The public identifier shall define the user's public address. The identifier shall be publicly available for the subscriber to allow that subscriber to be contacted. The private identifier shall only used within the network and is not publicly available.

The definition of the structure of the private identifier shall be modified slightly from that defined by 3GPP with the introduction of the use of the TMSI, P-TMSI as well as the IMSI for that identifier.

8.1 Public Identity

For the public identity, The SIP-IWF shall use the identifiers, unchanged, and as defined within the 3GPP specifications [3] The public identity shall define a publicly available identity for the subscriber of the UE that is being registered. The subscriber may also have a number of associated identities defined. These additional identities may be activated once the initial registration procedure is completed successfully.

The primary public identifier shall be based on the MSISDN of the UE, the additional identifiers, may utilise either the sip or tel URI format.

The MSISDN format of the public identity for a UE that has a UK MSISDN of 07863-119-343 is:

tel: +44-7863-119-343

The additional identities shall be passed to the IN-c device through the use of the P-Associated-URI header [8]. Examples of these are shown below:
sip:john.smith@ims vodafone.com

sip: +44-1223-815-540@orange.com

8.2 Private Identity

The private identity shall be used within the Authorization header of the SIP register message, and shall be the absolute identifier for the UE that is being registered

Three types of private identifier shall be defined for use with the SIP-IWF. The first identifier is the private identity that shall be based on the IMSI as defined in [3] and modified slightly here, the second identifier shall be based on the

TMSI and that is defined in this document along with the third identifier that shall be based on the P-TMSI.

The TMSI and P-TMSI shall be used as a private identifier in addition to the IMSI to allow the retrieval of security key information from the previous network node without a requirement to always return to the HLR/AuC for the authentication vectors.

The private identity of a UE based on the IMSI shall take the following format: <mcc><mnc><msin>.imsi@ ims.mncXXX mccYYY.3gppnetwork.org

As an example, a UE with MNC=015 (the MNC shall be represented as a 3 digit MNC, even if only two digits are used. In this case the leading digit is set to 0), MCC=234, MSIN=09999999999 would have the following NAI:
234150999999999.imsi@ims.mnc015.mcc234.3gppnetwork.org

The private identity of a UE based on the TMSI shall take the following format: <mcc><mnc><lac><tmsi>.tmsi@ ims. mncXXX.mccYYY.3gppnetwork.org

The lac is the location area code and is a 16 bit quantity represented as four lower-case hexadecimal digits The TMSI is a 32bit quantity that is represented as 8 lower-case hexadecimal digits. So the UE with the same MNC and MCC as previously, but with a LAC = 0x12ae and TMSI=0x82efd2ae would have the following private identity:
2341512ae82efd2ae tmsi@ims.mnc015.mcc234.3gppnetwork.org
The private identity of a UE based on the P-TMSI shall take the following format.
<mcc><mnc><lac><rac><p-tmsi>.ptmsi@ ims.
mncXXX.mccYYY 3gppnetwork.org

The rac is as the routing area code and is an 8 bit quantity represented as two lower-case hexadecimal digits. The P-TMSI is a 32bit quantity that is represented as 8 lower-case hexadecimal digits. So the UE with the same

MNC and MCC as previously, a LAC = 0x12ae, RAC = 2f and P-TMSI=0xeaf506db would have the following private identity: 2341512ae2feaf506db.ptmsi@ims.mnc015.mcc234.3gppnetwork.org

8.3 TMSI/P-TMSI Private Identity Allocation

After a successful Registration / Location/Routing area update, the new TMSI/P-TMSI shall be returned to the IN-c device and then on to the UE. The new TMSI/P-TMSI shall use the format defined in the previous section and returned as one of the P-Associated-URI entries.

9. Services

A range of services have been defined for the IN-c [2]. Here we will consider the message flows for each of the services that are required to be supported.

9.1 CS Call Scenarios

In this section we will consider the message flows for the circuit switched services. The SIP-IWF is used for the call control in the pre-IMS network. For the IMS-Ready network an S-CSCF and other IMS network elements are used.

The pre-IMS network and the IMS-ready network message flows are considered individually.

Two main call types are considered: a CS voice call and a CS video call. The voice call is MO and MT UE to the PSTN. The video call message flow considers a UE-UE call

An additional voice call, referred to as the home call is also described. The home call allows an incoming call to a defined home number, but the termination of that call could be any of the UEs currently registered on the IN-c device.

9.1.1 MO CS Voice Call Establishment – Pre-IMS Network

A CS MO voice call to the PSTN is considered here. The message flows are based on the 3GPP R5 IMS message flows. For the pre-IMS network, the support for the PRACK and UPDATE messages is [FFS] and some of the messages may be removed to allow compatibility with pre-IMS SIP gateway products.

1) The starts a MO call be requesting an RRC connection to the IN-c device.

2) The UE starts the voice call procedure by requesting an MM connection using the CM Service Request message.

3) The IN-c device shall request the activation of integrity protection and encryption (optional) using the Security Mode Command. The IN-c device shall know whether encryption is to be used based on a parameter IN-C-ENCRYPTION-ALGORITHM that is configured by the EMS

4) The UE acknowledges the request to activate integrity protection and encryption with the Security Mode Complete message.

5) The UE starts the procedure to establish the voice connection by sending the Setup message. The Setup message will include the necessary parameters to establish a call such as the dialled number and the type of call.

6) The IN-c device shall extract the necessary parameters from the Setup message and create a SIP INVITE request. The SIP INVITE request shall be sent to the SIP-IWF. The request shall include SDP parameters that define the media type, codec types, ports and QoS.

7) The SIP-IWF shall respond to the INVITE with a SIP 100 Trying response On receipt of the response, the IN-c device shall to stop any re-transmissions of the INVITE request.

8) The SIP-IWF shall respond indicating that the session is on-going by sending a SIP 183 Session Progress response. The 183 Session Progress shall include an SDP answer to the SDP offer received in step 5. The SIP-IWF shall indicate its preferred codec types in the SDP answer.

9) On receipt of the 183 Session Progress message, the IN-c device shall send the Call Proceeding message to the UE. The IN-c device shall store the SDP parameters to use when the media bearers are established.

10) To acknowledge the receipt of the 183 Session Progress response, the IN-c device shall send a SIP PRACK request to the SIP-IWF.

11) The SIP-IWF shall acknowledge the receipt of the SIP PRACK request by sending a SIP 200 OK response.

12) The IN-c device shall request the establishment of the radio bearers that are required to support the media. The IN-c device shall send the Radio Bearer Setup message to the UE. The message shall contain the details required by the UE to create a new radio bearer for the voice call.

13) The UE establishes the new Radio Bearer and responds with a Radio Bearer Setup Complete message.

14) When the radio resources are available and the QoS levels meet the required levels for the media connection at the UE end of the call, the SIP UPDATE request shall be sent from the IN-c device to the SIP-IWF.

15) On receipt of the SIP UPDATE request, the SIP-IWF shall proceed with the MT leg of the call by sending the SS7 ISUP INITIAL ADDRESS MESSAGE (IAM). The IAM message shall be sent to the PSTN to establish the terminating leg of the call.

16) The SIP 200 OK response shall be sent by the SIP-IWF to the IN-c device to acknowledge receipt of the UPDATE message.

17) The PSTN switch acknowledges the receipt of the call request and indicates the destination address is correct and the call is proceeding by sending the SS7 ISUP ADDRESS COMPLETE MESSAGE (ACM).

18) The SIP-IWF shall indicate to the IN-c device that the end terminal is available by sending the SIP 180 Ringing response.

19) The IN-c device shall indicate to the UE that the destination terminal is available by sending the ALERT message.

20) The IN-c device shall acknowledge the receipt of the SIP 180 Ringing response by sending a SIP PRACK request to the SIP-IWF

21) The SIP-IWF shall acknowledge the receipt of the PRACK with a SIP 200 OK request.

22) When the destination user accepts the incoming call, an SS7 ISUP ANSWER (ANM) message is sent to the SIP-IWF.

23) The SIP-IWF shall send the SIP 200 OK response message to the IN-c device. This indicates that the call is being connected.

24) The IN-c device shall send a Connect message to the UE indicating that the call is connecting.

25) The UE acknowledges that the call is going ahead with the Connect Ack.

26) The IN-c devices shall send the SIP ACK request to the SIP-IWF indicating that the call has connected.

27) The call continues until the UE attached to the IN-c device terminates the call.

28) When the call is completed, the UE ends the call. The DISCONNECT message is sent to the IN-c device.

29) The IN-c device shall send the SIP BYE request to the SIP-IWF.

30) The SIP-IWF shall acknowledge the BYE with the SIP 200 OK response.

31) The IN-c device shall send the Release message to the UE.

32) The SIP-IWF shall indicate the call is clearing by sending the Release message to the PSTN switch.

33) The Release Complete message is sent by the UE to the IN-c device to acknowledge the release of the call.

34) The PSTN switch sends the SS7 ISUP RELEASE COMPLETE (RLC) to indicate that the call is completed.

9.1.2 MT CS Voice Call Establishment– Pre-IMS Network

A CS MT originated voice call from the PSTN is considered here The message flows are based on the 3GPP R5 IMS message flows For the pre-IMS network the support for the PRACK and UPDATE messages is [FFS] and some of the messages may be removed to allow compatibility with non-IMS SIP gateway products.

1) The call is started by a user attached to the PSTN calling a UE attached to an IN-c device. The PSTN sends an SS7 ISUP INITIAL ADDRESS MESSAGE (IAM) to a GMSC in the IN-c network.

2) The GMSC will request routing information for the UE that is being called. The routing information is requested using the MAP Send Routing Information message. The request is sent to the HLR.

3) The HLR shall identify the SIP-IWF as the current location of the UE that is being called. The HLR will send the MAP Provide Roaming Number message to the SIP-IWF to request a roaming number that can be used to contact that UE.

4) The SIP-IWF shall allocate a roaming number and sends this to the HLR in a MAP Provide Roaming Number Ack message. The SIP-IWF shall store this roaming number in the local database.

5) The HLR sends the MAP Send Routing Information Ack message to the GMSC. The message contents include the roaming number that was provided by the SIP-IWF

6) The GMSC attempts to establish a call to the SIP-IWF by sending the SS7 ISUP INITIAL ADDRESS MESSAGE message it received previously.

7) The SIP-IWF shall forward the in-coming call request to the IN-c device using a SIP INVITE request. The INVITE request shall include SDP offer parameters that define the media type, preferred codec types, port numbers and QoS requirements.

8) The IN-c device shall respond to the SIP-IWF with a SIP 100 Trying response This response acknowledges the receipt of the INVITE request and terminates any re-transmissions of the INVITE by the SIP-IWF.

9) The IN-c device shall page the UE by sending a PAGING TYPE1 message over the paging channel

10-12) The UE requests the establishment of a radio connection between the IN-c device and the UE.

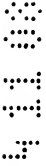
13) The UE acknowledges the paging request with the PAGING RESPONSE message.

14) The IN-c device shall start to activate integrity protection and encryption (optional) by sending the Security Mode Command. The IN-c device shall request encryption type defined by the parameter IN-C-ENCRYPTION-ALGORITHM that was configured by the EMS.

15) The UE acknowledges the start of integrity protection and ciphering with the Security Mode Complete message.

16) The IN-c device shall start to establish the call leg to the UE by sending the Setup message.

17) The UE acknowledges the receipt of the Setup message with the Call Confirmed message.



18) The IN-c device shall send the SIP 183 Session Progress request to the SIP-IWF. The request includes the SDP answer parameters selected by the IN-c device based on the offered SDP parameters received in the INVITE request. The IN-c device shall store the selected parameters for use when the bearers are to be configured.

19) The SIP-IWF shall acknowledge the receipt of the 183 Session Progress with the SIP PRACK request.

20) The IN-c device shall acknowledge receipt of the PRACK with the SIP 200 OK response.

21) The IN-c device shall request the UE to establish a radio bearer to carry the media for the connection to the UE from the IN-c device.

22) The UE acknowledges the establishment of the radio bearer with the Radio Bearer Setup Complete message.

23) When the radio bearer is active and operational, the IN-c device shall send a SIP UPDATE request to the SIP-IWF indicating that the QoS resources for the terminating end of the call are available.

24) The SIP-IWF shall acknowledge the receipt of the UPDATE request with the SIP 200 OK response.

25) The UE alerts the user to an incoming call and notifies the IN-c device with the Alerting message.

26) The IN-c device shall notify the SIP-IWF that the call is proceeding with the SIP 180 Ringing response.

27) The SIP-IWF shall acknowledge the receipt of the 180 Ringing message by sending the SIP PRACK request to he IN-c device.

28) The IN-c device shall acknowledge the receipt of the PRACK request with the SIP 200 OK response.

29) On receipt of the SIP 200 OK response, the SIP-IWF shall notify the GMSC that the call is proceeding by sending the SS7 ISUP ADDRESS COMPLETE message.

30) The GMSC forwards the ADDRESS COMPLETE message to the PSTN switch.

31) When the subscriber answers the call, the UE sends the Connect message to the IN-c device.

32) The IN-c device shall send the SIP 200 OK response to the SIP-IWF indicating the call started with the INVITE is proceeding.

33) The SIP-IWF shall acknowledge the SIP 200 OK response with the SIP ACK request.

34) The IN-c device shall acknowledge the receipt of the Connect with the Connect Ack. sent to the UE.

35) On receipt of the SIP 200 OK response, the SIP-IWF shall notify the GMSC that the call is connecting by sending the SS7 ISUP ANSWER message.

36) The GMSC forwards the ANSWER message to the PSTN switch.

37) The call continues until the subscriber attached to the IN-c device terminates the call.

38) The user on the UE terminates the call. The DISCONNECT message is sent to the IN-c device.

39) The IN-c device shall notify the SIP-IWF that the call is clearing by sending the SIP BYE request.

40) The SIP-IWF shall acknowledge the receipt of the BYE request by sending the SIP 200 OK response.

41) On receipt of the BYE request, the SIP-IWF sends the SS7 ISUP RELEASE to the GMSC.

42) The GMSC sends the SS7 ISUP RELEASE to the PSTN switch.

43) The IN-c device shall send the Release message to the UE.

44) The Release is acknowledged by the UE with the Release Complete message.

45) The PSTN acknowledges the SS7 ISUP RELEASE with the SS7 ISUP RELEASE COMPLETE sent to the GMSC.

46) The GMSC sends the SS7 ISUP RELEASE COMPLETE to the SIP-IWF.

9.1.3 MO CS Video Call Establishment – Pre IMS Network

A MO video call is illustrated here. The UE requests a bearer to transport the 64kb/s video

1) The UE requests the establishment of a CS Video call. The process starts with the establishment of an RRC connection

2) The UE requests an MM connection that it can use for the signalling of its video call attempt using the CM Connection Request message.

3) The IN-c device shall request the activation of integrity protection and encryption (optional) to the UE using the Security Mode Command. The keys used shall be based on the ones received during the registration procedure. The IN-c device shall request the encryption type defined by the parameter IN-C-ENCRYPTION-ALGORITHM that was configured by the EMS.

4) The UE acknowledges the activation of integrity protection and ciphering by sending the Security Mode Complete message to the IN-c device.

5) The UE requests the establishment of the video call by sending the Setup message to the IN-c device. The Setup message requests a 64kb/s synchronous bearer and includes the requirement for the H.223 and H.245 interworking function. This indicates that a CS H.324M multimedia connection is being requested.

6) The IN-c device shall request the establishment of a CS data connection using a SIP INVITE request. The INVITE, sent to the SIP-IWF, shall include the SDP offer parameters that request the establishment of a data connection with a data rate for the connection of 64kb/s

7) The SIP-IWF shall acknowledge the INVITE with a SIP 100 Trying response.

8) The SIP-IWF shall respond to the INVITE with a SIP 183 Session Progress response that includes the SDP answer to the previous offered parameters from the IN-c device.

9) The IN-c device shall inform the UE that the call is proceeding.

10) The IN-c device shall acknowledge the receipt of the 183 Session Progress by sending a SIP PRACK request to the SIP-IWF.

11) The SIP-IWF shall acknowledge the receipt of the PRACK by sending the SIP 200 OK response.

12) The IN-c device shall request the UE to establish a radio bearer to support the video call by sending the Radio Bearer Setup message.

13) After the UE has established the radio bearer, it acknowledges that the radio bearer has been created with the Radio Bearer Setup Complete message

14) When the resources match the required QoS for the video connection, the IN-c device shall send the SIP UPDATE request to the SIP-IWF

15) The SIP-IWF shall start the establishment of the terminating leg of the call be sending the SS7 ISUP INITIAL ADDRESS MESSAGE to the GMSC of the network where the connection is being established.

16) The SIP-IWF shall acknowledge the UPDATE message with the SIP 200 OK response

17) The GMSC requests the location information and roaming phone number for the UE from the HLR using the MAP Send Routing Information message

18) The HLR requests the MSC to which the UE is attached to provide a roaming number that can be used by the GMSC to address the UE that is terminating the call.

19) The MSC controlling the UE responds with a roaming number in the MAP Provide Roaming Number Ack message back to the HLR.

20) The HLR passes the roaming number back to the GMSC via the MAP Send Routing Information Ack message

21) The GMSC can now send the SS7 ISUP INITIAL ADDRESS MESASAGE to the MSC that is controlling the UE.

22) The UTRAN at the request of the MSC will now page the UE. The Paging Type1 message will be from the SRNC, but is shown as being from the MSC for simplicity.

23-25) A radio connection and then a signalling connection to the UE is established

26) The UTRAN establishes a security context to the UE. Integrity protection and ciphering (optional) are activated using the Security Mode Command.

27) When the security context is established the UE acknowledges its creation with a Security Mode Complete message

28) The MSC requests the UE to establish a call by sending a Setup message. The Setup message will request the establishment of a 64kb/s bearer and includes the use of the H 223 and H.245 interworking function to support the H.324M video call.

29) The UE acknowledges the call establishment request be sending the Call Confirmed message to the MSC.

30-31) The UTRAN requests the establishment of a RAB to carry the video media across the radio interface.

32) When the RAB is established the UE responds with the Alert message to the MSC indicating that the user is being altered to the incoming video call.

33) The MSC indicates that the call is proceeding to the GMSC using the SS7 ISUP ADDRESS COMPLETE MESSAGE.

34) The SS7 ISUP ADDRESS COMPLETE MESSAGE is forwarded to the SIP-IWF by the GMSC.

35) The SIP-IWF shall notify the IN-c device that the call is proceeding using the SIP 180 Ringing response.

36) The IN-c device shall send the Alert message to the UE. The message alerts the originating UE to the progress of the call.

37) The IN-c device shall acknowledge the receipt of the 180 Ringing by sending a SIP PRACK request to the SIP-IWF.

38) The SIP-IWF shall acknowledge the receipt of the PRACK with the SIP 200 OK response.

39) The call is accepted by the terminating UE. The Connect message is sent to the MSC by the UE.

40) The SS7 ISUP ANSWER message is sent to the GMSC by the MSC. This notifies the GMSC that the call connection has been received.

41) The MSC sends a Connect Ack to the UE indicating that the Connect was received correctly.

42) The GMSC sends the SS7 ISUP Answer message to the SIP-IWF to notify it that the call connection has occurred.

43) The SIP-IWF shall send a 200 OK message to the IN-c device to indicate that the call connection has occurred.

44) The IN-c device shall sends a Connect to the UE. Both ends of the call leg are now connected.

45) The UE acknowledges the Connect by sending a Connect Ack to the IN-c device.

46) The IN-c device shall notify the call completion to the SIP-IWF by sending the SIP ACK request.

47) The SIP-IWF shall inform the GMSC of the call completion by sending the SS7 ISUP CONNECT ACK message to the GMSC.

48) The two UEs enter into a second stage of call establishment using the H.245 protocol to negotiate and establish the H.324M video call within the bearer that has been created. This signalling is end-to-end and does not require any intervention from the intervening core network. The call continues until the UE attached to the IN-c device terminates the call.

49) The call is terminated by the UE attached to the IN-c device with the DISCONNECT message being sent to it.

50) The IN-c device shall notify the SIP-IWF that the call is being terminated by sending the SIP BYE request.

51) The SIP-IWF shall acknowledge the receipt of the BYE message by sending the SIP 200 OK response to the IN-c device.

52) The IN-c device shall notify the UE that the call disconnect is accepted by sending the Release message.

53) The UE acknowledges the Release message by sending the Release Complete message to the IN-c device.

54) The SIP-IWF shall notify the GMSC that the call is being terminated by sending an SS7 ISUP RELEASE message to the GMSC.

55) The GMSC notifies the MSC that the call is being released by sending an SS7 ISUP RELEASE message.

56) The MSC notifies the UE that the call is terminated by sending the Release message to the UE.

57) The UE acknowledges the receipt of the call termination with the Release Complete message.

9.1.4 MT CS Home Call Establishment

This call scenario is to a number that is associated with the IN-c device (the "home number") rather than to a specific UE. The call flows are basically the same as a normal MT call, except that the paging is performed in sequence to all UEs starting with the master user if present. The paging sequence stops as soon as there is a response to the paging message from a UE. If the call isn't established to that UE, (e.g. no answer after a defined number of rings), the paging process may start again.

A simple scenario is illustrated in Figure 39.

Although the scenario illustrated below is specifically shown for the pre-IMS network, the same methodology applies to the IMS-Ready network, with the SIP-IWF replaced by the S-CSCF or equivalent node from the IMS network

1-8) An incoming call to the number that is defined as the "home number" starts. The call establishment is the same as a normal MT call (as defined previously) until the call arrives at the IN-c device.

9) The IN-c device shall recognise the incoming call as that of the home. The IN-c device shall start to establish a call to the UEs that are active and registered on the IN-c device. The paging for the calls will start according to user priority as defined by either the operator or the master user.

10) The IN-c device tries successive paging attempts to all of the UEs attached to the IN-c. The paging message to UE number n is sent to the network.

11) The paging request to UE number n is successful. This UE responds to the paging request with an RRC Connection Setup indicating that it is responding to the paging message.

12) The remainder of the MT call establishment continues as normal and as defined elsewhere.

9.1.5 MO CS Voice Call Establishment – IMS-Ready Network

The following call scenario presents the call establishment from a UE attached via an IN-c device to an IMS-Ready network. In the call flows that follow, the IN-c device takes the role of both the UAC and the P-CSCF It is an implementation decision as to whether the IN-c device contains both the UAC and the P-CSCF provided the messaging appears that both are present in the signalling path.

1) The MO call attempt starts with the UE establishing a radio connection to the IN-c device.

2) The UE requests the establishment of an MM connection to carry the call signalling connection to the IN-c device using the CM Service Request message.

3) The IN-c device shall initiate the activation of integrity protection and encryption (optional) using the Security Mode Command The IN-c device shall request the encryption type defined by the parameter IN-C-ENCRYPTION-ALGORITHM that was configured by the EMS.

4) The UE acknowledges the establishment of the security context to the IN-c device by sending the Security Mode Complete message to the IN-c device.

5) To initiate the call, the Setup message is sent from the UE to the IN-c device. The Setup message will indicate the characteristics of the call to be established. In this instance it is a speech call using the AMR codec.

6) The IN-c device on receipt of the Setup message shall start to establish a SIP session to the IMS. A SIP INVITE request is sent to the S-CSCF. The INVITE message includes the SDP offered parameters that define the characteristics of media for the call. The SDP parameters will include media type, a selection of preferred codecs, the port number and the required QoS.

7) The S-CSCF forwards the SIP INVITE request to the MGCF that interfaces to the CS PSTN.

8) The S-CSCF acknowledges the INVITE request to the IN-c device by sending the SIP 100 Trying response.

9) The MGCF acknowledges the receipt of the INVITE request to the S-CSCF by sending a SIP 100 Trying response.

10) The MGCF selects the codec type from the received list in the SDP parameters and responds to the S-CSCF with a 183 Session Progress message including the selected set of SDP parameters in the SDP answer to the SDP offer. The SDP parameters included by the MGCF will include the preferred codec, the port numbers to use for the media and the current QoS status at the terminating end of the link.

11) The 183 session progress is forwarded to the IN-c device by the S-CSCF.

12) The IN-c device shall indicate to the UE that the call is going ahead by sending the Call Proceeding message.

13) The IN-c device shall acknowledge the receipt of the 183 Session Progress by sending a PRACK request to the S-CSCF. The IN-c device shall store the answered SDP parameters received in the 183 Session Progress response.

14) The S-CSCF forwards the SIP PRACK request to the MGCF.

15) The MGCF acknowledges the receipt of the PRACK with the SIP 200 OK response sent to the S-CSCF.

16) The S-CSCF forwards the SIP 200 OK response to the IN-c device.

17-18) The IN-c device shall establish the radio bearer to the UE using the Radio Bearer Setup procedures

19) After the radio bearer is established the IN-c device shall send an UPDATE request to the S-CSCF. The UPDATE shall indicate that the local end QoS resources are available for the connection.

20) The S-CSCF forwards the SIP UPDATE request to the MGCF.

21) If the remote end QoS resources are available, the MGCF responds to the UPDATE with a SIP 200 OK response.

22) The SS7 ISUP INITIAL ADDRESS MESSAGE is sent to the PSTN switch indicating that there is an incoming call.

23) The S-CSCF forwards the SIP 200 OK response to the IN-c device acknowledging the UPDATE and the QoS resource allocation.

24) The PSTN switch indicates that the end user terminal is available and has been alerted to an incoming call be sending the SS7 ISUP ADDRESS COMPLETE MESSAGE to the MGCF.

25) The MGCF indicates that the end terminal is proceeding with the call by sending the SIP 180 Ringing response to the S-CSCF.

26) The S-CSCF forwards the 180 Ringing response to the IN-c device.

27) The IN-c device on receipt of the 180 Ringing response shall send the Alert message to the UE

28) The IN-c device shall send a SIP PRACK request in acknowledgement of receipt of the SIP 180 Ringing response. The PRACK is sent to the S-CSCF.

29) The S-CSCF forwards the SIP PRACK request to the MGCF.

30) The MGCF acknowledges the receipt of the PRACK by sending the SIP 200 OK response to the S-CSCF.

31) The S-CSCF forwards the SIP 200 OK response to the IN-c device.

32) When the terminating user accepts the incoming call, the SS7 ISUP ANSWER MESSAGE (ANM) is sent from the PSTN switch to the MGCF

33) The MGCF indicates to the S-CSCF that the call connection has been established by sending the SIP 200 OK response to the original INVITE.

34) The S-CSCF forwards the 200 OK to the IN-c device.

35) On receipt of the 200 OK, the IN-c device shall send a Connect message to the UE indicating that the call connection has been established.

36) The UE acknowledges the receipt of the Connect message by sending the Connect Ack message to the IN-c device.

37) The IN-c device shall acknowledge that the connection is established by sending an ACK to the S-CSCF.

38) The S-CSCF forwards the ACK to the MGCF.

39) The call between the UE and the terminal connected to the PSTN continues until the call is terminated by the UE.

40) On termination of the call, the UE sends the Disconnect message to the IN-c device

41) Upon receipt of the Disconnect from the UE, the IN-c device shall send a SIP BYE request to the S-CSCF.

42) The S-CSCF forwards the SIP BYE request to the MGCF.

43) On receipt of the BYE, the MGCF sends the SS7 ISUP RELEASE (REL) message to the PSTN switch.

44) The MGCF acknowledges the receipt of the BYE by sending the SIP 200 OK response to the S-CSCF.

45) The S-CSCF forwards the SIP 200 OK to the IN-c device.

46) On receipt of the 200 OK, the IN-c device shall send a Release message to the UE.

47) The UE acknowledges the receipt of the Release message by sending the Release Complete message to the IN-c device.

48) The PSTN switch acknowledges the receipt of the Release by sending an SS7 ISUP RELEASE COMPLETE (RLC) message to the MGCF

9.1.6 MT CS Voice Call Establishment – IMS Ready Network

The following call scenario presents the call establishment from a terminal attached to the PSTN to a UE that is attached to an IN-c device in an IMS-Ready network. In the call flows that follow, the IN-c device takes the role of both the UAC and the P-CSCF. It is an implementation decision as to whether the IN-c device contains both the UAC and the P-CSCF provided the messaging appears that both are present in the signaling path.

In the IMS-Ready network, it is assumed that the MGCF knows the S-CSCF to which the UE is attached. In a more general case the I-CSCF may be used to locate the S-CSCF where the UE is located. This doesn't not impact the message flows as far as the IN-c device is concerned and so it is not considered further.

1) The terminal attached to the PSTN originates a call. The SS7 ISUP Initial Address Message (IAM) is sent to the MGCF by the PSTN switch. The IAM will include the destination number for the call, in this case the registered address of the UE.

2) The MGCF creates the SIP INVITE request in response to the IAM. The INVITE will include the initial SDP offer parameters. The SDP parameters will include the media type, preferred codec list, port numbers and QoS requirements.

3) The S-CSCF acknowledges the receipt of the SIP INVITE request and sends a SIP 100 Trying response back to the MGCF.

4) The S-CSCF forwards the SIP INVITE request to the IN-c device.

5) The IN-c device shall acknowledge the INVITE by sending a SIP 100 Trying response to the S-CSCF.

6) The IN-c device shall start to page the UE with a Paging Type1 message.

7) The UE responds to the paging request. The UE initiates the procedure to create a radio connection to the IN-c device

8) When the radio connection is available, the UE sends a paging response to the IN-c device indicating that the signalling connection is present and available.

9) The IN-c device shall establish a security context to the UE using the Security Mode Command. The security context includes the activation of integrity protection and encryption (optional) The IN-c device shall request the encryption type defined by the parameter IN-C-ENCRYPTION-ALGORITHM that was configured by the EMS.

10) The UE acknowledges the establishment of the security context by sending the Security Mode Complete message to the IN-c device.

11) The IN-c device shall start the procedure to establish the call to the UE by sending the Setup message to the UE. The Setup message shall provide the details of the call including the selected codec.

12) The UE acknowledges the receipt of the Setup by sending the Call Confirmed message to the IN-c device.

13) The IN-c device shall notify the S-CSCF that the call is proceeding by sending a 183 Session Progress response. The SIP 183 Session progress response will include SDP answer to the SDP offer contained in the INVITE request. The SDP parameters shall indicate the choice of codecs based on the original list, the port number for the media and the status of the QoS resources

14) The S-CSCF forwards the SIP 183 Session Progress response to the MGCF

15) The MGCF acknowledges the receipt of the 183 Session Progress by sending the SIP PRACK request to the S-CSCF.

16) The S-CSCF forwards the SIP PRACK request to the IN-c device.

17) The IN-c device shall acknowledge the receipt of the SIP PRACK request by returning a SIP 200 OK response to the S-CSCF.

18) The S-CSCF forwards the SIP 200 OK response to the MGCF.

19) When the QoS resources in the Media Gateway (not shown) are available for the call, the MGCF sends the SIP UPDATE request to the S-CSCF. The UPDATE will indicate via the SDP parameters that the resources defined by the QoS at the originating end of the link are available.

20) The S-CSCF forwards the SIP UPDATE request to the IN-c device.

21) The IN-c device, on receipt of the UPDATE, shall start to establish the radio bearer that will be used to carry the media by sending the Radio Bearer Setup to the UE.

22) When the radio bearer has been established, the UE sends the Radio Bearer Setup Complete message to the IN-c device.

23) When the QoS resources are available at the UE end of the link, the SIP 200 OK response to the UPDATE shall be sent by the IN-c device to the S-CSCF. The 200 OK will include the SDP parameters that have been modified to include the QoS status at the terminating end of the link.

24) The S-CSCF forwards the SIP 200 OK response to the MGCF.

25) As the call proceeds the UE alerts the subscriber to the incoming call and sends the Alerting message to the IN-c device.

26) On receiving the Alerting message from the UE, the IN-c device shall send a SIP 180 Ringing response to the S-CSCF.

27) The S-CSCF forwards the SIP 180 Ringing response to the MGCF.

28) The MGCF acknowledges the SIP 180 Ringing response be sending a SIP PRACK request to the S-CSCF.

29) The S-CSCF forwards the SIP PRACK request to the IN-c device

30) The IN-c device shall acknowledge the PRACK request with the SIP 200 OK response sent to the S-CSCF.

31) The S-CSCF forwards the SIP 200 OK response to the MGCF.

32) The MGCF on receipt of the SIP 200 OK response for the PRACK generates an SS7 ISUP Address Complete Message (ACM). The ACM is sent to the PSTN switch and indicates that the call is proceeding and the terminating terminal is alerting the subscriber.

33) When the subscriber answers the call the Connect message is sent from the UE to the IN-c device

34) The IN-c device on receipt of the Connect shall send the SIP 200 OK response to the S-CSCF. The 200 OK is in response to the original INVITE and indicates that the connection has been created.

35) The S-CSCF forwards the SIP 200 OK response to the MGCF.

36) The MGCF on receipt of the SIP 200 OK response sends an SS7 ISUP answer message to the PSTN switch.

37) The MGCF acknowledges that the connection is proceeding by sending the SIP ACK request to the S-CSCF.

38) The MGCF forwards the SIP ACK request to the IN-c device.

39) The IN-c device on receipt of the SIP ACK request shall send the Connect Ack to the UE.

40) The call can now proceed with the media flowing from the UE to the IN-c device and then onto the Media Gateway. The UE terminates the call.

41) On call termination, the UE sends a Disconnect message to the IN-c device.

42) On receipt of the Disconnect message, the IN-c device shall send a SIP BYE request to the S-CSCF.

43) The S-CSCF forwards the SIP BYE request to the MGCF.

44) The MGCF sends the SS7 ISUP RELEASE message to the PSTN switch.

45) The MGCF acknowledges the receipt of the SIP BYE request sending a SIP 200 OK response to the S-CSCF.

46) The S-CSCF forwards the SIP 200 OK response to the IN-c device.

47) The IN-c device on receipt of the SIP 200 OK response shall generate a Release message which is sent to the UE.

48) The UE acknowledges the Release by returning a Release Complete message to the IN-c device.

49) The PSTN switch acknowledges the SS7 ISUP RELEASE from the MGCF by returning an SS7 ISUP RELEASE COMPLETE message (RLC).

9.2 Packet Data Services

In this section the packet data services to the CN are considered.

9.2.1 Packet Access to Operator Specific Data Services

Packet access to operator specific data services shall be achieved through the use of an IPSec tunnel to the PDG, and from there into the operator's data network. This is illustrated in the message flow presented in Figure 42. As an IPSec tunnel has previously been created, the authentication information is available in the AAA server for the second IPSec tunnel.

1) The UE requests the establishment of a PDP context to allow access to packet data services in the operators network. The Activate PDP Context Request message is sent to the IN-c device. The APN in the request will indicate that it is for access to the operator specific data services.

2) The IPSec security associations establishment is now started with the exchange of information that will be used to establish the security associations. The information includes cryptographic algorithm negotiation, exchange of nonces and a Diffie Hellman exchange. The IN-c device shall send an IKEv2 IKE_SA_INIT message to the TTG. The message includes the security association and nonces.

3) The TTG shall return an IKEv2 IKE_SA_INIT message including the security association parameter and nonces.

4) The IN-c device shall send an IKE_AUTH_REQUEST message to permit the TTG to authenticate the IN-c device. The contents of the message shall include the IMSI of the IN-c device, the request to configure the tunnel, details of the security associations and the operator services APN.

5) The TTG shall send a DIAMETER-EAP-Request message carrying a null EAP message, but including the IMSI of the IN-c device.

6) The AAA server shall check to see if an AV and profile are available.

7) The AAA server shall responds with a DIAMETER-EAP-Success message indicating that the IN-c device has previously been authenticated and the previously derived Master Session Key can be used. The Master Session Key shall be passed to the TTG for use in generating the cryptographic keys.

8) The TTG shall send an EAP identity request message to the AAA server to check that the IN-c device is allowed to create a tunnel to the endpoint defined by the APN.

9) The AAA server checks to see if the IN-c device is allowed to access the services given by the APN

10) The AAA server shall acknowledges that the tunnel to the endpoint can be created.

11) The TTG shall send a Create PDP Context Request message to the GGSN via the Gn' interface.

12) The GGSN sends a Create PDP Context Response message to the TTG. The message includes the IP address allocated by the GGSN for the tunnel.

13) After receipt of the Diameter-AA-Answer message, the TTG shall compute the AUTH parameter for the first and second IKE-SA-INIT messages. These two messages were sent without integrity protection, and so the MSK shall be used to generate this authentication parameter.

14) The TTG shall send an IKE_AUTH_RESPONSE message to the IN-c device. The purpose of this message is to carry the EAP_Success indicating the successful request to establish a tunnel.

15) The IN-c device shall send an IKE_AUTH_REQUEST message to authenticate the IN-c device prior to establishing the tunnel. The message includes the AUTH parameter that is computed based on the IN-c derived master session key.

16) The TTG shall respond with the IKE_AUTH_RESPONSE that includes the AUTH parameter, the CFG_REPLY parameter and the security association parameter. The AUTH parameter is used to authenticate the IKE_SA_INIT message. The Remote IP address is passed to the IN-c device. The Remote IP address is the inner IP address that will be used in the tunnel between the IN-c device and the TTG. On completion, the secure tunnel between the IN-c device and the TTG will be ready.

17) A SIP INVITE request shall be sent to the SIP-IWF from the IN-c device. The INVITE shall indicate that a data session between the IN-c device and the GGSN is being created. The reason for the INVITE is to ensure that the SIP-IWF is aware that the data session is active should a handover to the macro cell occur, and session continuity is required. The INVITE shall include SDP parameters that define a data session

18) The SIP-IWF shall respond with a SIP 200 OK response.

19) The IN-c device shall acknowledge the 200 OK response with a SIP ACK request.

20) The IN-c device shall notify the UE that the PDP context is established by sending it an Activate PDP Context Accept message.

21) The tunnel is established between the IN-c device and the TTG. A second GTP tunnel is established between the TTG and the GGSN. The AAA server knows the IP address associated with the tunnel, and so billing for the premium data services can be associated with the IMSI of the IN-c device. The IN-c device shall be responsible for encapsulating the data going into the tunnel and providing the session keys that are derived from the Master session key.

9.2.2 Packet Access to Internet

A simpler form of packet data access is to access the Internet data services directly from the IN-c, this is illustrated in Figure 43.

1) The UE requests the establishment of a radio connection and signalling connection to the IN-c device.

2) The UE requests the establishment of a GMM context that can be used for the signalling and the establishment of the PDP context by sending the Service Request message.

3) The Security Mode Command shall be sent by the IN-c device to the UE to establish a security context between the UE and the IN-c device. The security context will include integrity protection and, optionally, encryption. The IN-c device shall request the encryption type defined by the parameter IN-C-ENCRYPTION-ALGORITHM that was configured by the EMS.

4) The UE acknowledges that the security context has been established with a Security Mode Complete message.

5) The UE requests the establishment of a PDP Context to the IN-c device using the Activate PDP Context Request message. The context request will

include the requested QoS and the APN for the desired end-point. The APN will be pre-configured by the EMS.

6) The IN-c device shall request the establishment of a radio bearer using the Radio Bearer Setup message.

7) Once the radio bearer is established, the UE acknowledges that the radio bearer is established by sending a Radio Bearer Setup Complete message to the IN-c device.

8) The IN-c device shall acknowledge the establishment of the PDP Context by sending the Activate PDP Context Accept message. The IN-c device shall allocate an IP address within a sub-net controlled by the IN-c and shall then be responsible for NATing that IP address to the external IP address assigned to the IN-c device by the backhaul service provider.

9.3 MO & MT SMS Transfer Scenarios

In this section we will consider two main SMS scenarios, the MO SMS transfer, and the MT SMS transfer. For UE to UE SMS transfer, with UEs located on the same IN-c, a loop-back procedure that does not require interaction with the SIP-IWF may be performed.

9.3.1 MO SMS Transfer

1) The UE sends the SMS message to the IN-c device. The message is contained within an RP-DATA message that is carried to the IN-c device encapsulated within the CP-DATA message.

2) The IN-c device shall acknowledge the receipt of the CP-DATA message by sending the CP-ACK message.

3) The IN-c device shall acknowledge the receipt of the RP-DATA message by sending the RP-ACK message encapsulated within a CP-DATA message.

4) The UE acknowledges the receipt of the CP-DATA message by sending a CP-ACK message.

5) The IN-c device shall send the SMS message within a SIP MESSAGE request. The SIP MESSAGE shall be sent to the SIP-IWF. From the SIP-IWF the SMS shall be sent to the IN-c network.

6) The SIP-IWF shall acknowledge the receipt of the SIP Message by sending a 200 OK response.

9.3.2 MT SMS Transfer

1) The SIP-IWF shall forwards an SMS message it has received for the UE using a SIP MESSAGE request to the IN-c device.

2) The IN-c device shall acknowledge the receipt of the message using a 200 OK response.

3) The IN-c device shall forward the SMS message to the UE in an RP-DATA message that is encapsulated within a CP-DATA message.

4) The UE acknowledges the CP-DATA message by sending a CP-ACK message.

5) The UE acknowledges the receipt of the RP-DATA by sending an RP-ACK encapsulated within a CP-DATA message.

6) The IN-c device shall acknowledge the CP-DATA message by sending a CP-ACK message to the UE.

10. Radio Resource Management

Control of resources utilised by the IN-c device can be divided into two groups. Resources that are controlled by the IN-c device and resources controlled by the IN-c network.

10.1 IN-c Device RR Management

10.1.1 Physical Layer RR Control Parameters

The physical layer radio resource parameters are considered here.

10.1.1.1 Scrambling Code Allocation Procedure

The scrambling code for the IN-c device shall be allocated pseudo-randomly by the IN-c device. The procedure for allocating the scrambling code on power up and on a periodic bases therein shall be as follows:

- Create Set A, a set of scrambling codes from all available scrambling codes received as configuration information from the IN-c network
- Randomly select one scrambling code from Set A.
- Cycle through all scrambling codes in Set A adding them in groups as neighbour cells in broadcast information and configure all UEs in the vicinity to report neighbour cell measurements on either PRACH channel or dedicated channel. If at any point the scrambling code selected by the IN-c device is reported as being used, select a different scrambling code from Set A.
- For each measurement report received:
- Create a Set B of scrambling codes for each IN-c device (CPICH power < 20dBm) located by the UE, add path loss estimate to Set B, remove the scrambling code from Set A.
- Create a Set C for each macro cell scrambling code located by the UE, add path loss estimate to Set C, remove scrambling code from Set A.
- Select scrambling code in the following order, stop procedure when one selected.
- Select pseudo-randomly the scrambling code from any remaining in Set A **OR:**
- Select the scrambling code with the largest path loss from Set B **OR:**
- Select the scrambling code with the largest path loss from Set C.

10.1.1.2 Cell Detection Function

The detection of the cells surrounding the IN-c device is required for a variety of purposes such as transmit power setting and location detection. A number of algorithms are proposed here to facilitate this depending upon the type of cell to be detected. The cell types are either intra frequency cells, inter-frequency cells or inter-RAT cells.

10.1.1.2.1 Intra-Frequency Cell Detection Function

The scrambling code, cell-identity and cell measurements for the intra-frequency cells surrounding the IN-c device shall be estimated using the following procedure.

1. Create Set A, a set of scrambling codes from all available scrambling codes.

2 Cycle through all scrambling codes in Set A taking them in groups of 32 Load the group as the list of intra-frequency neighbour cells into the broadcast message SIB11/SIB12 then:

a. For each UE that accesses the IN-c device extract the measurements that are made on the PRACH and/or the dedicated channel.

b. Repeat for N_UE_ATTEMPTS measurement reports by the UE.

c. For each scrambling code reported, add the scrambling code, cell identity and measurements to the intra-frequency-cell-list, and delete the scrambling code from the SET A.

d. Get the next group of scrambling codes from SET A.

3. Repeat from step 3 until no additional cells are detected for any of the remaining scrambling codes.

10.1.1 2.2 Inter-Frequency Cell Detection Function

The scrambling code, cell-identity and cell measurements for the inter-frequency cells surrounding the IN-c device shall be estimated using the following procedure.

1. Select first UARFCN from the set of alternate UARFCNs provided by the EMS.

2. Create Set A, a set of scrambling codes from all available scrambling codes.

3. Cycle through all scrambling codes in Set A taking them in groups of 32. Load the group as the list of intra-frequency neighbour cells into the broadcast message SIB11/SIB12 then:

a. For each UE that accesses the IN-c device extract the measurements that are made on the PRACH and/or the dedicated channel.

b. Repeat for N_UE_ATTEMPTS measurement reports by the UE.

c For each scrambling code reported, add the UARFCN, scrambling code, cell identity and measurements to the inter-frequency-cell-list, and delete the scrambling code from the SET A.

d Get the next group of scrambling codes from SET A.

4. Repeat from step 3 until no additional cells are detected for any of the remaining scrambling codes.

5. Repeat from step 2 selecting the next UARFCN in the list

10.1.1.2.3 Inter-RAT Cell Detection Function

This function applies specifically to GSM cell detection. The detection of other RATs such as CDMA2000 is [FFS]. The BSIC, frequency, cell-identity and cell measurements for the inter-RAT cells surrounding the IN-c device shall be estimated using the following procedure.

1. Create Set A, a set of valid BCCH ARFCNs codes received from the EMS. Select four ARFCNs from Set A.

2. For each selected ARFCN create 8 entries in the inter-RAT cell list within the SIB11/SIB12 broadcast message, one for each BSIC (NCC is fixed and set by EMS, BCC has 8 possible values) then:

a. For each UE that accesses the IN-c device extract the measurements that are made on the PRACH and/or the dedicated channel.

b. Repeat for N_UE_ATTEMPTS measurement reports by the UE.

c. For each ARFCN/BSIC reported, add the UARFCN, BSIC, cell identity and measurements to the inter-RAT-cell-list, and delete the ARFCN from the SET A.

d. Select the next four ARFCNs from SET A and repeat 2.

3. Repeat from step 1 until no additional cells are detected for any of the remaining ARFCNs.

10.1.1.3 Cell transmit power setting

The IN-c device shall be configured by the IN-c network with an absolute maximum transmit power that it can use (P_{Tmax}).

The IN-c device receives neighbour cell power measurements from the UEs within its coverage area. based on these power measurements, the IN-c device shall set its transmit power such that the required coverage area is achieved, with the minimum transmit power P_T.

In the power setting algorithm P_T shall always be less than P_{Tmax}.

10.1.1.4 Channelisation code allocation

The channelisation codes shall be allocated dynamically based on the number of users that are active at any instant in time.

10.1.1.5 Admission control functions

The admission control function in the IN-c device maintains a permanent record of the resources that are committed within the IN-c device. Should a request for new resources come from a new UE entering the coverage area,

the admission control function shall only grant the request for resources if they are available.

10.2 IN-c Network RR Management

The RR management functions in the IN-c network shall comprise a set of configurable parameters that can be modified through the management system The Configurable parameters have a default value that is used to when an IN-c device makes a request to be configured and also a dynamic value that can be changed by the operator.

11. Network Management

The two new managed nodes in the IN-c network shall be the IN-c device and the SIP-IWF. The other entities within the IN-c network are standard components within the 3GPP network architecture and do not require consideration here.

Two management protocols shall be used for managing the IN-c device. The first is the IETF based SNMP protocol and the second is the DSL Forum TR69 protocol [16]. The IN-c device shall support both of these protocols, the SIP-IWF shall support SNMP only.

11.1 SNMP Based Management

The IN-c device and the SIP-IWF shall both support the SNMP protocol for element management, they both shall contain an SNMP agent. The EMS shall contain the SNMP manager

A MIB is defined for the IN-c device The MIB shall be located in the IN-c device and the EMS shall be used to define the parameters that may be configured or audited by the EMS.

11.1.1 Configuring IN-c Device on Initial Activation

On power-up and at any point thereon, the EMS may reconfigure the IN-c device. Either all of the configuration parameters defined in the IN-c device MIB, or a selected sub-set of parameters may be configured.

11.1.1.1 Procedure for Configuring IN-c Device

The EMS shall use the SNMP command setRequest to set each parameter. The IN-c device shall respond with the getResponse message to indicate the receipt of the setRequest. For a larger number of parameters the sequence shall be repeated sequentially. The process is illustrated in Figure 46.

11.1.1.2 Data Configured in IN-c Device

The data that may be configured in the IN-c device is outlined in the table below along with an explanation for what the data is and why the data may need to be configured.

Parameter(s)	IN-c Device Access [1]	EMS Access	Comment
MIB (Master Information Block)	R	R/W	The PLMN Identity will be depend upon the operator and will be configured at installation.
SIB3	R	R/W	The cell selection and re-selection criteria affect how the UE finds a cell. These parameters can be configured by the EMS.
SIB5	R/W	R	The common channel parameters will vary dynamically
SIB 11	R/W	R	Set of neighbour macro-cells on same frequency, different frequency, GSM cells.

[1] This is direct access by the IN-c device and does not include the access via the EMS to this data that is stored on the IN-c device.

Operating UARFCN	R	R/W	The UARFCN that the IN-c device should use is defined by this parameter.
Alternative UARFCNs	R	R/W	A set of alternative UARFCNs that the operator uses for their network are provided to allow measurements on the macro network cells to be made.
RNC-Id	R	R/W	The identifier for the "virtual" RNC used by the IN-c device for the cell identifier.
Primary scrambling code set	R	R/W	The set of allowed primary scrambling codes that the IN-c device may select from
Selected scrambling code	R/W	R	The scrambling code selected by the IN-c device
NCC	R	R/W	Network colour code used by operator for GSM BSIC.
ARFCNs	R	R/W	Set of ARFCNs to search for GSM cells.
Max Tx Power	R	R/W	The maximum allowed Tx power set by the EMS
P-CPICH Tx Power	R/W	R	The CPICH Tx power selected by the IN-c device
Postcode	R	R/W	The postcode of the house where the IN-c device is located, this is set by the IN-c device based on information obtained when the unit was purchased.
LAI	R	R/W	Location area identifier for the IN-c device. This is configured by the EMS
RAI	R	R/W	Routing area identifier for the IN-c device. This is configured by the EMS.
PLMN-ID	R	R/W	This is the PLMN-Id for the IN-c device, this is configured by the EMS

Intra-Frequency-Cell-List	R/W	R	The cell identity and scrambling code for the set of intra-frequency cells that the IN-c device has received in measurements from the UEs. The list will also include the measurement values for each entry.
Inter-Frequency-Cell-List	R/W	R	The cell identity and scrambling code for the set of inter-frequency cells that the IN-c device has received in measurements from the UEs. The list will also include the measurement values for each entry.
Inter-RAT-Cell-List	R/W	R	The cell identity and frequency for the set of inter-RAT cells that the IN-c device has received in measurements from the UE. The list will also include the measurement values for each entry.
RNC-IDs	R	R/W	A database of RNC-ID : LAI/RAI : SIP-IWF : MSC-ID : SGSN : S-CSCF : E-CSCF- used by IN-c device for the purposes of location information.
Serving SIP-IWF	R/W	R/W	SIP-IWF selected by IN-c device based on the location information
Serving-MSC	R/W	R/W	MSC to be used for emergency calls
Serving SGSN	R/W	R/W	SGSN to use for emergency calls (for future use)
IMSIs & IMEIs	R/W[c][2]	R/W	Database of IMSIs allowed access to IN-d device including date of last access to IN-c device. List of IMEIs can be associated with each IMSI.

[2] This is conditional on whether it is user access control or operator access control in the parameter UE_ACCESS_CONTROL

TMSIs	R/W	R	TMSI associated with any UE on IN-c device
Master user IMSI and IMEIs	R/W[c]	R/W	Defines the IMSI and IMEIs associated with the master user. This is used for home calling even if it is operator defined UE access.
AVs	R/W	R ?	Current authentication vector associated with each registered IMSI
S-CSCF	R/W	R/W	Identity of the S-CSCF that the IN-c device will use for accessing the IMS
EMS	R/W	R/W	Identity of the EMS used to configure the IN-c device.
Active UEs	R/W	R	List of IMSIs currently active on IN-c device
In-Service-Flag	R/W	R/W	Flag that defines whether the IN-c Device is allowed to be in-service or not.
RTT List	R	R/W	A list of URLs or IP addresses to be used by the IN-c device to estimate Round Trip Times (RTT) using the Ping function.
RTT Values	R/W	R	A database of statistics for the RTTs from the RTT list These values are used within the location awareness function
N_UE_ATTEMPTS	R	R/W	Defined the number of measurements that a UE should make of adjacent cells before trying different codes.
Home phone number	R	R/W	A phone number that is configured for the IN-c device that will page any registered UEs in the home, and which can be used as the identifier for any emergency calls originating from the IN-c device.

Tunnel_Control_Param	R	R/W	Defines the tunnel allocation strategy. Options misght include: Single tunnel, 3 separate tunnels: control, cs servces, ps services, one tunnel per service, fixed BW tunnels and new tunnels when aggregate exceeded.
IN-c Device Access Gating (IMEI or IMSI)	R	R/W	Defines whether the IMEI is used for gating or just the IMSI.
UE_ACCESS_CONTROL	R	R/W	Defines whether the operator or the user provide the list of IMSIs that gate access to the IN-c device.
UE direct Internet access	R	R/W	Defines whether the UE is allowed to go straight out to the Internet or not. If the IE us allowed direct Internet access, the IN-c device shall provision an APN in the UE for this purpose, when the UE is first accesses the IN-c device.
UE access operator data services	R	R/W	Defines whether the UEs are allowed to access operator specific services via the IN-c device.
Tunnel Types	R	R/W	Defines what types of tunnels are allowed. Same as control, per service, QoS controlled
Boot URL	R	R/W	Defines the URL of the boot network entity. It will contact this device after the DHCP has allocated an IP address. The URL shall be stored in the USIM.
UE_ACCESS_REJECT_TYPE1	R	R/W	Defines the reject cause for some LAU/RAUs
UE_ACCESS_REJECT_TYPE2	R	R/W	Defines different reject cause if PLMN-Id same as macro PLMN-Id
SIP-IWF-REGISTER	R	R/W	Defines whether registration to the SIP-IWF is required in the IMS-Ready network

IDLE_MODE_SELECT_TYPE	R	R/W	Defines the type of Idle Mode selection methodology. HPLMN different to macro PLMN or HPLMN same as macro PLMN-ID, but using RAI for reject.
IN-C-ENCRYPTION-ALGORITHM	R	R/W	Defines which encryption algorithm shall be used: None, UEA1, ...

Table 5: Data Accessible by EMS and IN-c Device

11.1.2 Auditing IN-c Device

The auditing of the IN-c device by the EMS shall be achieved through the SNMP getRequest and getResponse commands. The getRequest defines the identity of the parameter to be audited and the getResponse shall contain the parameter value. An example of this procedure for a number of sequential parameters is illustrated in Figure 47.

11.1.3 Event Reporting in IN-c Device

The SNMP protocol manages errors and events through the use of traps. If an event occurs within the IN-c device, the IN-c device shall generate a trap that is sent to the EMS. The trap shall contain a trap identifier and also some additional information that may be used to manage the event.

An example of an event is illustrated in Figure 48.

11.1.4 Configuring SIP-IWF

[TBD]

11.2 TR69 Based Management

[TBD]

12. Billing and Charging

12.1 IN-C Device Derived Billing

The IN-c device shall generate billing information. The generation of billing information shall be for a number of session types. The different session types are outlined below.

- PS data direct Internet access.
- PS data 3GPP IP access
- CS external service.
- CS internal service (local switching).
- SMS or MMS message exchange.

For some of these services additional billing information shall be derived by the IN-c network. In these cases, the information derived by the IN-c device is supplemental to that information. The usage of the supplemental information is an operator issue.

To generate the billing information, the IN-c device shall support both the RADIUS and the DIAMETER protocols. The IN-c device shall send RADIUS/DIAMETER accounting messages to the AAA server. The AAA server will forward these messages to the CDF via the Wf interface. The interface between the AAA server is DIAMETER based and consequently the AAA server will be required to convert between RADIUS and DIAMETER in the case when the RADIUS is used across the Wa interface.

The message flow for the billing related to the establishment and termination of a session is illustrated in Figure 49. In the message flow, the support for both DIAMETER and RADIUS is illustrated together.

1. The service to be billed is started.

2. The IN-c device shall send a DIAMETER/RADIUS Accounting Request message that indicates that the service has started. A session ID is allocated

by the IN-c device and included in the message to identify the session to be billed.

3. The AAA server converts the RADIUS message to a DIAMTER message and forwards it to the CDG.

4. The CDG acknowledges the request for CDRs with the DIAMETER Accounting Answer message that includes a parameter Account Interim Interval (AII) that defines how frequently interim billing information is passed to the CDG.

5. The AAA server passes the Accounting Answer message to the IN-c device. For RADIUS based Wa interface this becomes an Accounting Response message.

6. The CDG creates a CDR that will be used to record the session charging details.

7. At the period defined by the AII, the IN-c device shall generate an interim record message and pass it to the AAA server via the Accounting Request message.

8. The AAA server forwards the Accounting Request message to the CDG.

9. The CDF acknowledges the interim record with the Accounting Answer message sent to the AAA server.

10. The AAA server forwards the Accounting Answer to the IN-c device, converting to RADIUS is required.

11. The CDG updates the CDR to reflect the data received in the interim record.

12. The session is stopped in the IN-c device.

13. The IN-c device shall send a Stop record to the AAA server via the Accounting Request message.

14. The AAA server forwards the Accounting Request message to the CDG.

15. The CDG closes the CDR for the session.

16. The CDG sends an Accounting Answer message to the AAA server.

17. The AAA server forwards the Accounting Answer message to the IN-c device, converting it to RADIUS equivalent if required.

12.2 PDG Derived Billing

The billing derived by the PDG (TTG + GGSN) is transferred to the Charging Gateway Function (CGF) via the Ga interface. The procedures and interface is identical to the PS domain.

The billing derived by the PDG will be for all data services that pass through the PDG. If the IN-c network is configured accordingly, these services may include CS voice and video services in addition to the PS data services accessed via the PDG.

An example of a message flow for a session being billed by the CGF is illustrated in Figure 50

1. The service to be billed is started.

2. The PDG sends the data record packet to the CGF

3. The CGF acknowledges the packet.

4. The session ends.

5. The PDG sends the final data record packet.

6. The CGF acknowledges the receipt of the data record packet.

13. Emergency Call Handling

The handling of Emergency Calls is slightly different between the Pre-IMS network and the IMS-Network. The emergency call will utilise some of the location information that is described later in this document.

The emergency call function shall only be available for UEs that are registered on the IN-c device.

13.1 Pre-IMS Network

The emergency call is illustrated Figure 51. The call establishment is essentially the same as the normal voice call, except that the destination routing of the call is modified by the IN-c device.

1) The UE initiates an emergency call in the normal manner, dialling the appropriate emergency number (e.g. 112, 911, etc). The call establishment to the IN-c device proceed as normal.

2) The IN-c device shall extract the dialling number of the closest emergency services centre from the local database. The number is defined, based on the RNC-ID of the macro-cells surrounding the IN-c device, or the LAI/RAI of the cells surrounding the IN-c device. The originating number for the emergency call shall be given as the home phone number as provisioned by the EMS and stored in the local database

3) The IN-c device shall send the initial INVITE to the SIP-IWF. The originating and destination addresses are as defined in step 2.

4) The SIP-IWF shall establish a CS connection to the emergency call centre. The number for the call centre is shall be provisioned by the EMS and corresponds the geographically closest number. The originating number for the emergency call shall be be the number associated with the registered location of the IN-c device. The operator's database for this number shall also include the address and postcode information for that location.

5) The emergency call proceeds as normal. On completion, the call terminates in the usual manner.

13.2 IMS-Ready Network

For the IMS-Ready network the emergency call shall be the same as a normal call, except the node in the IMS core shall be the E-CSCF instead of the S-CSCF.

The address of the E-CSCF shall be stored in the database in the IN-c device when the device is initially configured, periodically and after a location change. The calling party identity for the emergency call shall be the home phone number as configured by the EMS.

14. Supplementary Services

14.1 Calling Line Identity Functions (CLIP/CLIR)

The CLIP/CLIR supplementary service shall be supported in both the IN-c device and the SIP-IWF.

An inbound call from an external network will include the calling line identity and an indication on the presentation of the calling line identity. The SIP-IWF will either transfer the calling line identity to the IN-c device using the INVITE request, or it will mask the identity according to RFC 3323 [44] The IN-c device will respond to the INVITE by replacing the appropriate fields in the SETUP message that is sent to the UE.

For the outbound CLIP/CLIR requirements the UE will indicate that the calling line identity is to be either presented or restricted. This information shall be passed to the IN-c device in the Setup message. The IN-c device shall pass this information to the SIP-IWF via the INVITE message as previously, with the considerations to privacy applied according to RFC 3323 [44].

14.2 Call Forwarding Unconditional (CFU)

The CFU supplementary service allows the subscriber to forward incoming calls to a different number. The user will request this service either through the keypad or via a menu option on the UE.

14.2.1 Activation of CFU

The activation of the CFU supplementary service is illustrated in Figure 52.

1) The subscriber (via the UE) requests the activation of the CFU supplementary service.

2) The UE sends the Register message to indicate that the CFU service is being requested.

3) The IN-c device shall convert the CFU request into an INVITE. The Request-URI line of the INVITE will be used to define the details of the CFU request according to Appendix C of [43].

4) The SIP-IWF shall interpret the INVITE request as a CFU activation request. A 183 session progress response is sent to the IN-c device.

5) The SIP-IWF shall send a Register message to the HLR indicating that a CFU request is being made. The details of the request are contained in the Register message.

6) The HLR acknowledges the Register with a Register Ack that is sent to the SIP-IWF.

7) The SIP-IWF acknowledges that the Register was received with the 200 OK sent to the IN-c device.

8) The In-c device sends the Release Complete message to the UE indicating that the CFU activation was successful

9) The IN-c device shall send a CANCEL request to the SIP-IWF to cancel the dialogue that was being created.

14.2.2 Call Forward Example from PSTN

1) An incoming call to the UE arrives from the PSTN to the UE that has CFU active.

2) The Initial Address Message (IAM) is sent to the GMSC from the PSTN.

3) The GMSC requests routing information for the UE from the HLR.

4) The HLR sends the routing information acknowledgement to the GMSC.

5) The GMSC forwards the Initial Address Message to the destination PSTN where the call is being forwarded.

6) The call establishment continues.

14.3 Call Forwarding on Mobile Subscriber Busy (CFB)

The CFB supplementary service allows the forwarding of a call to a different destination in the case when the subscriber is busy.

14.3.1 Activation of CFB

1) The subscriber (via the UE) requests the activation of the CFB supplementary service.

2) The UE sends the Register message to indicate that the CFB service is being requested.

3) The IN-c device shall convert the CFB request into an INVITE. The Request-URI line of the INVITE will be used to define the details of the CFU request according to Appendix C of [43].

4) The SIP-IWF shall interpret the INVITE request as a CFB activation request. A 183 session progress response is sent to the IN-c device.

5) The SIP-IWF shall send a Register message to the HLR indicating that a CFB request is being made. The details of the request are contained in the Register message.

6) The HLR acknowledges the Register with a Register Ack that is sent to the SIP-IWF

7) The SIP-IWF acknowledges that the Register was received with the 200 OK sent to the IN-c device.

8) The In-c device sends the Release Complete message to the UE indicating that the CFB activation was successful

9) The IN-c device shall send a CANCEL request to the SIP-IWF to cancel the dialogue that was being created

14.3.2 Call Forward Example from PSTN

1) An incoming call to the UE arrives from the PLMN1 to the UE that has CFB active.

2) The Initial Address Message (IAM) is sent to SIP-IWF from the PLMN.

3) The SIP-IWF discovers that the UE is in a call, and the call shall be forwarded.

4) The to SIP-IWF requests call forwarding information for the UE from the HLR.

5) The HLR sends the call forwarding information acknowledgement to the SIP-IWF.

6) The SIP-IWF forwards the Initial Address Message to the destination PSTN where the call is being forwarded.

7) The call establishment continues.

14.4 Call Waiting (CW)

The CW supplementary service allows a subscriber to be notified that there is an incoming call whilst in an on-going call. The subscriber may accept the new call in preference to the on-going call, keep the ongoing-call on hold or reject the new call.

14.4.1 Activation of CW

1) The subscriber (via the UE) requests the activation of the CW supplementary service.

2) The UE sends the Register message to indicate that the CW service is being requested.

3) The IN-c device shall convert the CW request into an INVITE. The Request-URI line of the INVITE will be used to define the details of the CW request according to Appendix C of [43]

4) The SIP-IWF shall interpret the INVITE request as a CW activation request. A 183 session progress response is sent to the IN-c device.

5) The SIP-IWF shall send a Register message to the HLR indicating that a CW request is being made The details of the request are contained in the Register message.

6) The HLR acknowledges the Register with a Register Ack that is sent to the SIP-IWF.

7) The SIP-IWF acknowledges that the Register was received with the 200 OK sent to the IN-c device.

8) The In-c device sends the Release Complete message to the UE indicating that the CW activation was successful.

9) The IN-c device shall send a CANCEL request to the SIP-IWF to cancel the dialogue that was being created.

14.4.2 Call Waiting Example

1) The subscriber has a call in progress via the IN-c device.

2) A new call comes in from the PSTN to the UE attached to the IN-c device (the interactions via the GMSC are not shown).

3) The SIP-IWF shall indicate to the IN-c device that there is an incoming call. The INVITE will include SDP parameters to establish a media path. The media path will be used initially for the transportation of the call waiting tone.

4) The IN-c device shall indicate to the UE that the call is being established via the Setup message The Setup message shall include a "Signal Information" element with value #7 to request the generation of a call waiting tone.

5) The UE responds with a Call Confirmed with cause information indicating that the user is busy.

6) The UE will send an Alert message indicating that the call waiting tone is being activated.

7) The IN-c device shall send a 182 Queue response to the SIP-IWF The response includes the SDP parameters that complete the negotiations over the media path that may be used for the call waiting tones.

8) The Address Complete message is sent to the originating switch. This will include the notification message that indicates that the call is waiting.

The call will proceed from this point in a number of ways. The new call may be: dropped, put on hold or accepted. The existing call may equally be dropped, put on hold or rejected.

14.5 Call Hold (HOLD)

The HOLD supplementary service allows a subscriber to put a call on hold, and at a later point either terminate the call or retrieve the call.

14.5.1 Activation of Call Hold

1) The subscriber (via the UE) requests the activation of the HOLD supplementary service.

2) The UE sends the Register message to indicate that the HOLD service is being requested.

3) The IN-c device shall convert the HOLD request into an INVITE. The Request-URI line of the INVITE will be used to define the details of the HOLD request according to Appendix C of [43].

4) The SIP-IWF shall interpret the INVITE request as a HOLD activation request. A 183 session progress response is sent to the IN-c device.

5) The SIP-IWF shall send a Register message to the HLR indicating that a HOLD request is being made. The details of the request are contained in the Register message.

6) The HLR acknowledges the Register with a Register Ack that is sent to the SIP-IWF.

7) The SIP-IWF acknowledges that the Register was received with the 200 OK sent to the IN-c device.

8) The In-c device sends the Release Complete message to the UE indicating that the HOLD activation was successful.

9) The IN-c device shall send a CANCEL request to the SIP-IWF to cancel the dialogue that was being created.

14.5.2 Call Hold Example

1) The subscriber has previously requested the establishment of a call to the PSTN

2) The subscriber requests that the call be put on hold. The UE sends a Hold message to the IN-c device.

3) The IN-c device shall acknowledge the receipt of the Hold with the Hold Acknowledge message

4) The IN-c device sends a (re-) INVITE request message to the SIP-IWF. The SDP parameters in the INVITE indicate that the media shall become send only (no media to be sent from the remote PSTN end of the link). The IN-c device shall stop the transfer of media from the local end.

5) The SIP-IWF shall respond with a 200 OK indicating that media will be receive only from the remote end

6) The IN-c device shall acknowledge the 2 OK response with a SIP ACK.

7) The SIP-IWD sends the SS7 ISUP Call Progress message. The contents of the message include the notification element that indicates that the call is being put on hold.

8) The subscriber requests the removal of the hold.

9) The UE sends the Retrieve message to recall the call.

10) The IN-c device shall acknowledge the call retrieval with the Retrieve Acknowledge message sent to the UE.

11) The IN-c device shall send a (re) INVITE message to the SIP-IWF indicating in the SDP parameters that the media is now send and receive.

12) The SIP-IWF shall respond with the 200 OK including the SDP parameters that acknowledge the return of the call.

13) The IN-c device shall send the SIP ACK to acknowledge the 200 OK.

14) The SIP-IWF shall send the SS7 ISUP Call Progress message to indicate that the call hold has been released.

14.6 Explicit Call Transfer (ECT)

The ECT supplementary service allows a subscriber to transfer a call from one subscriber to another subscriber.

14.6.1 Activation of Explicit Call Transfer

1) The subscriber (via the UE) requests the activation of the ECT supplementary service.

2) The UE sends the Register message to indicate that the ECT service is being requested.

3) The IN-c device shall convert the ECT request into an INVITE. The Request-URI line of the INVITE will be used to define the details of the ECT request according to Appendix C of [43].

4) The SIP-IWF shall interpret the INVITE request as a ECT activation request. A 183 session progress response is sent to the IN-c device.

5) The SIP-IWF shall send a Register message to the HLR indicating that a ECT request is being made. The details of the request are contained in the Register message.

6) The HLR acknowledges the Register with a Register Ack that is sent to the SIP-IWF.

7) The SIP-IWF acknowledges that the Register was received with the 200 OK sent to the IN-c device.

8) The In-c device sends the Release Complete message to the UE indicating that the ECT activation was successful.

9) The IN-c device shall send a CANCEL request to the SIP-IWF to cancel the dialogue that was being created.

14.6.2 Explicit Call Transfer Example

In this example of the Explicit Call Transfer a single MSC is shown controlling the two UEs that are receiving the call from the UE1 The procedure will apply equally if there are two MSCs controlling the call.

1) The subscriber is in two calls. The call to UE2 is on hold and the call to UE3 is active. The subscribers requests the Explicit Call Transfer SS which will result in the calls to UE1-UE2 and UE1-UE3 being dropped, and call UE2-UE3 being established.

2) UE1 sends a Facility message indicating ECT is requested to the IN-c device.

3) The IN-c device shall send a REFER request to the SIP-IWF which requests that the call leg UE1-UE2 and UE1-UE3 be connected and UE1 leave the call.

4) The SIP-IWF acknowledges the REFER request with the 202 Accepted response.

5) The SIP-IWF shall send the SS7 ISUP Call Progress message to the MSC controlling UE2 to indicate that it is being taken off hold and that an ECT is in progress.

6) The MSC sends a Facility message to the UE2 to indicate that the UE is being retrieved from hold, and that an ECT is in progress.

7) The SIP-IWF shall send the SS7 ISUP Call Progress message to indicate that an ECT is in progress to the MSC that controls UE3.

8) The MSC sends a Facility message indicating that the ECT is in progress to UE3.

9) UE3 responds with a Connect message to the MSC indicating that the new connection is active.

10) The MSC sends the SS7 ISUP Answer message to the SIP-IWF indicating that the call transfer is proceeding.

11) The MSC acknowledges the receipt of the Connect from UE3 by sending a Connect Ack back to UE3.

12) The SIP-IWF shall send a SIP NOTIFY message to the IN-c device to indicate that the transfer is complete.

13) The IN-c device shall acknowledge the NOTIFY by sending the SIP 200 OK response to the SIP-IWF.

14) The IN-c device closes the dialogues with the SIP-IWF by sending the BYE request. (This is sent twice, one for each dialogue, but only shown once in the diagram).

15) The SIP-IWF shall acknowledge the receipt of the BYEs by sending 200 OKs.

16) The IN-c device shall send a Disconnect message to the UE to indicate the connection is being closed.

17) The UE shall acknowledge the Disconnect with a Release message.

18) The IN-c device shall acknowledge the Release with a Release Complete message.

15. Quality of Service Management

15.1.1.1 Diffserv Codepont

Table below presents the mapping relationship between the UMTS QoS classes and the Diffserv codepoints (DSCP) that shall be used in the ToS field in the IP packet header

3GPP Traffic Class	Priority	Diffserv PHB	DSCP	Typical Service
Conversational	-	EF	101110	VoIP, Video conferencing
Streaming	-	AF4	100010	Audio / Video streaming
Interactive	1	AF3	011010	Gaming
	2	AF2	010010	Web browsing
	3	AF1	001010	Telnet
Background	-	BE	000000	E-mail, Download

Table 6: QoS Traffic Classes mapping to Diffserv Codepoints

15.2 IN-c Device QoS Management

The IN-c device shall ensure for all services that are established that the packet marking shall be according to the classification outlined in Table 6 above.

When queuing the packets onto the backhaul, the IN-c device shall give higher priority to the conversational class. The Assured Forwarding (AF) PHB shall be queued and shaped according to a RED algorithm and the Best Effort PHN allocated any spare capacity as and when it comes available.

15.3 IN-c Network QoS Management

The IN-c transport network shall support Diffserv from the backhaul access point to the destination point.

16. Software Download Functions

Software download shall be via an FTP server located within the EMS. The software download function shall be controlled via the EMS and will occur in stages.

Stage 1. Software to support the boot process and IN-c authentication procedure.

Stage 2: Remainder of software to support the complete IN-c device application

The IN-c device shall have sufficient permanent memory to store two complete software images The first image will be the working copy that is only over-written when a new image has been successfully downloaded and tested as being fully functional.

17. Lawful Intercept Functions

The SIP-IWF shall support lawful intercept using the standard interfaces and protocols.

18. Location Awareness Functions

The location awareness function is responsible for managing data associated with.the location of the IN-c device. The location awareness function is used by a number of other functions. The object of the location awareness function is to maintain state information as to the current location of the IN-c device and to detect if the location of the IN-c device has changed

There are five data elements to the location awareness function.

- Postcode for location of IN-c device entered into database in IN-c network when unit purchased or updated via help-desk if unit moved to new location. Downloaded whenever new configuration information passed to IN-c device
- Linked list of RNC-IDs, LAIs, SIP-IWF IDs and MSC-Ids.
- List of Cell-Ids and statistics measured by UE.
- RTT magnitude statistics for a number of defined URLs and IP addresses.
- LAI/RAI identification through updates.

18.1.1 Setting Initial Location Values

During the initial configuration of the IN-c device, or after a location change event has been detected, the location values shall be computed and stored.

18.1.1.1 Postcode Data Setting

The postcode setting for the IN-c device is configured by the EMS. On initial activation, this is the value that obtained at the point of sale and identifies the geographic location of the IN-c device. If the IN-c device is detected as being moved, the postcode data will need to be updated via a help desk function.

18.1.1.2 RNC-Identity List

After the IN-c device has been activated for the first time, and after a location change has been detected, the EMS will download a set of RNC-Ids and associated with each one an identity for a SIP-IWF, an MSC, an SGSN and a S-CSCF.

When the first set of cells are found and identified by the IN-c device as part of the initial activation procedure for the IN-c device, the RNC-Id of the cells can be obtained from the Cell-Id for the cells. From the RNC-Id, the IN-c device will be able to define which SIP-IWF to use, which MSC to use for emergency calls and which S-CSCF to use.

18.1.1.3 Cell Fingerprint Measurement

Upon initial activation, or after a location change event, the IN-c device will characterise the RF environment in which it sits by creating a "fingerprint" of the surrounding cells. The IN-c device shall request any UEs that come into the coverage area to measure all of the neighbour cells that are on the same frequency, a different frequency or a different system (such as GSM).

When the measurement reports are made, the IN-c device builds a database of measurements that include the cell identity, UARFCN used, the path loss measurement, Ec/No measurement, RSCP measurement and SFN-SFN time offset measurement. This set of information can be used to create a fingerprint of the radio environment in which the IN-c device is located. The UE may need to make periodic changes to these measurements to account for seasonal variations and changes in the operational characteristics of these cells It is unlikely, however, that all of the measurements from all of the cells would change instantaneously, unless the IN-c device was moved to a different location.

18.1.1.4 RTT Fingerprint Measurement

Upon initial activation, or after a location change event, the IN-c device will characterise the RTT environment in which it sits by creating a "fingerprint" of known IP addresses.

Using the IP ping protocol and a list of URLs and IP addresses configured in the IN-c device by the EMS, the IN-c device can measure the statistics of the RTT between the IN-c device and the target IP node. Using these measurements that IN-c device can create a database that will be used as a fingerprint for its location.

18.1.1.5 LAI/RAI Identification Function

In poor coverage areas there may be no surrounding macro cells that the UE can measure. In this scenario the IN-c device shall monitor the LAI / RAI that are used to identify the UE when it attempts to register on the IN-c device. By maintaining a database of previously used LAI/RAIs, the IN-c device can establish the LAI/RAI that is closest to the location of the IN-c device. From this LAI/RAI and the data configured by the EMS, the IN-c device has an approximate estimate as to its location.

18.1.2 Location Change Detection Function

The location change detection function is responsible for detecting when the IN-c device has been moved. There are three basic types of movement that may occur and which are listed below:

- Intra-residence – a change in the location of the IN-c device within the residence of the subscriber
- Intra-network – a change in the location of the IN-c device but still within the same network.
- Inter-country – a change in the location of the IN-c device involving a change in the country of operation of the device.

18.1.2.1 Intra-Residence Location Change Detection

18.1.2.1.1 IN-c Device within Coverage Area of Surrounding Macro Cells

The location change caused by the movement of the IN-c device within the subscriber's residence will be detected by a sudden step change in the measurements that the UE makes for the surrounding cells. The step change will be predominantly to the measurements of the path loss, RSCP and Ec/No. There may be a slight change to the detected cell list.

On detecting an intra-residence location change, the IN-c device will recreate the database for the cell fingerprint. No location change event will be generated.

18.1.2.1.2 IN-c Device outside the Coverage Area of Surrounding Macro Cells
Although not a commonly occurring, there is a possibility that the IN-c device is outside the coverage area, and there are no other cells detectable on any frequency or any system. IN this instance, the RTT fingerprint shall be used to detect a change in location.

The RTT fingerprint measures the average RTT between the IN-c device and a set of known servers on the internet. The average value will remain approximately the same when measured over a long time period. No change in the RTT time for a significant number of the connections will suggest that the location of the IN-c device is the same.

18.1.2.2 Intra-Network Location Change Detection

18.1.2.2.1 IN-c Device within Coverage Area of Surrounding Macro Cells
A change in location of the IN-c device, but still within the coverage of the macro cell can be detected by a sudden change in the identity of the cells being reported by the UEs to the IN-c device. The IN-c device will know the RNC-Identity of the new area from the detected cell identities found by the UE, and consequently the SIP-IWF, MSC and S-CSCF that should be used are also known from the configuration information received from the EMS.

18.1.2.2.2 IN-c Device outside the Coverage Area of Surrounding Macro Cells
Although not a commonly occurring, there is a possibility that the IN-c device is outside the coverage area, and there are no other cells detectable on any frequency or any system. In this instance, the RTT fingerprint shall be used to detect a change in location.

18.1.2.3 Inter-Country Location Change Detection

18.1.2.3 1IN-c Device within Coverage Area of Surrounding Macro Cells

A change in country will result in a change in the available PLMNs. As a consequence of this, the UE will not receive any cell measurements as the PLMN-ID will be incorrect.

In this instance, the RTT fingerprint shall be used to detect a change in location.

18.1.2.3.2IN-c Device outside the Coverage Area of Surrounding Macro Cells

In this instance, the RTT fingerprint shall be used to detect a change in location.

18.1.3 Location for Emergency Calls

To support the emergency call functions, the IN-c device shall include location information in all emergency calls established to the SIP-IWF.

The emergency call location information shall include postcode, RNC-Id, MSC-Id, Cell Id and SIP-IWF Id.

The emergency call location information shall be obtained by correlating the RNC-Id obtained from the neighbour cells, with the list of RNC-Ids received from the EMS.

19. Prevention of Roaming Fraud

Roaming fraud shall be detected using the location change detection functions. If a location change is detected and the location change is inter-country, the IN-c device shall report the change as an event to the EMS.

The EMS shall then set the IN-Service-Flag to indicate that the IN-c device is out-of-service.

20. Power on Self Test

The IN-c device shall include a power-on diagnostic test The tests performed by the IN-c device shall include.

- Processor test.
- Memory test (permanent and temporary).
- Ethernet interface test.
- Radio test.
- Software checksum test.

On completion of the power-on self test, the IN-c device shall initiate the IN-c device authentication procedures.

CLAIMS

1 A method of determining if a 3G access point has been moved, comprising the step of measuring features of the network environment in which the access point is located to create a fingerprint, and determining that the access point is moved if there is a significant change to the fingerprint.

2 A method according to claim 1, wherein the step of creating a fingerprint comprises:

requesting any user equipment within a coverage area of the access point to measure properties of neighbouring cells and report the measurement to the access point; and

building a database of the measurements, that includes cell identity, UTRAN absolute radio frequency channel number (UARFCN), path loss, Ec-No, received signal code power (RSCP), and system frame number – system frame number (SFN-SFN) time offset, to create the fingerprint.

3. A method according to claim 1, wherein the step of creating a fingerprint comprises:

characterising the round trip time (RTT) environment in which the access point is located by creating a database of measurements of the round trip time between the access point and plurality of known IP addresses.

4. A method according to claim 1, wherein the step of creating a fingerprint comprises:

monitoring the location area identifier (LAI) or routing area identifier (RAI) that is used to identify a user device when it attempts to register with the access point, and maintaining a database of previously used LAIs or RAIs to establish the LAI or RAI closest to the access point.

INTELLECTUAL PROPERTY OFFICE

167

Application No: GB0619892.3 **Examiner:** Mr Richard Howe

Claims searched: 1-4 **Date of search:** 4 January 2009

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	1	WO2008/051124 A1 Ericsson - see abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art
Y	Document indicating lack of inventive step if combined with one or more other documents of same category	P	Document published on or after the declared priority date but before the filing date of this invention
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X]:

Worldwide search of patent documents classified in the following areas of the IPC

H04Q; H04W

The following online and other databases have been used in the preparation of this search report

Online : wpi ; epodoc

International Classification:

Subclass	Subgroup	Valid From
H04W	0004/00	01/01/2009
H04W	0004/02	01/01/2009
H04W	0004/04	01/01/2009
H04W	0016/00	01/01/2009
H04W	0028/00	01/01/2009
H04W	0040/00	01/01/2009
H04W	0040/04	01/01/2009
H04W	0080/00	01/01/2009